1(1) 2026

Open Access

Interdisciplinary Journal of Computing & AI

IJCAI
Interdisciplinary Journal of Computing & AI

Mohuya Chakraborty *Editor-in-chief*

Publisher: Aspiration Publishing Trust
not-for-profit organization

30 April 2026

Volume 1 | Issue 1 | 2026

Interdisciplinary Journal of Computing & AI

Mohuya Chakraborty *Editor-in-chief*

Publisher: Aspiration Publishing Trust

not-for-profit organization

30 April 2026

Interdisciplinary Journal of Computing & AI

IJCAI

IJCAI
Interdisciplinary Journal of Computing & AI

PREFACE

It is with great pride and enthusiasm that we present the inaugural issue of the Interdisciplinary Journal of Computing & AI (IJCAI). This launch represents a significant milestone in our shared vision to foster high-quality, interdisciplinary research that bridges computing, artificial intelligence, and emerging technological domains. As the boundaries between disciplines continue to dissolve, platforms like IJCAI become essential in cultivating innovation that addresses complex, real-world challenges.

A notable highlight of this inaugural issue is that all published papers are indexed in OpenAIRE. This achievement underscores our strong commitment to global open science principles—ensuring visibility, accessibility, and transparency in research dissemination. By aligning with international academic standards, IJCAI aspires to serve as a credible and impactful forum for scholars, practitioners, and researchers worldwide.

The contributions in this issue reflect both diversity and depth, covering a wide range of contemporary topics. These include predictive analytics for heart failure readmission risk, advancements in GPU power management and optimization, and AI-driven biometric-secured virtual try-on systems. The issue also features innovative work on blockchain-enabled federated learning platforms for privacy-preserving insights and creator reward mechanisms, alongside research on cyber-physical systems with post-quantum security frameworks. Further, it highlights interdisciplinary applications of AI in rural water governance and privacy-preserving communication systems within India's cybersecurity ecosystem.

Collectively, these works demonstrate the transformative potential of integrating computing and AI across domains such as healthcare, cybersecurity, and engineering systems. They exemplify how interdisciplinary collaboration can lead to meaningful solutions that are both technologically advanced and socially relevant.

We extend our sincere gratitude to all authors for their valuable contributions, the reviewers for their rigorous evaluation and constructive feedback, and the editorial team for their unwavering dedication in bringing this issue to fruition. Their collective efforts have laid a strong foundation for the journal's future.

As IJCAI embarks on its academic journey, we are confident that it will evolve into a globally recognized platform for impactful research and intellectual exchange. We look forward to its continued growth and its role in shaping the future of interdisciplinary innovation.

We wish the journal every success in its pursuit of academic excellence and global relevance.

Editorial Board
Interdisciplinary Journal of Computing & AI (IJCAI)
Inaugural Issue, 2026

Copyright & Publication Information

Journal: Interdisciplinary Journal of Computing & AI | Volume 1, Issue 1, April 2026

Publisher: Aspiration Publishing Trust — a registered not-for-profit academic publishing trust focused on elevating interdisciplinary research and supporting academic communities.

Publisher Address: Sree, 150, Motijheel Avenue, Dum Dum Kolkata 700074, West Bengal, India

https://doi.org/10.5281/zenodo.19674476

Open Access | Indexing: OpenAIRE

Message from the Patron

It gives me immense pleasure to present the inaugural issue of the Interdisciplinary Journal of Computing & AI (IJCAI). This launch marks a significant milestone in our mission to promote high-quality, interdisciplinary research at the intersection of computing, artificial intelligence, and emerging technologies. We are particularly proud that all papers in this inaugural issue are indexed in OpenAIRE, ensuring enhanced visibility, accessibility, and alignment with global open science standards. This achievement reflects our commitment to transparency, research dissemination, and international academic integration. The contributions featured in this issue represent a diverse spectrum of cutting-edge research, including:

- Predictive analytics for heart failure readmission risk from the University of Ohio, USA,
- GPU power management and optimization from NIT Jamshedpur, India,
- AI-driven biometric-secured virtual try-on systems from Thakur College of Engineering and Technology, India,
- Blockchain-enabled federated learning platforms for privacy-preserving ad preference insights and creator reward mechanisms, from the University of Engineering and Management, Kolkata, India,
- Cyber-physical and post-quantum secure control innovations from Amity University, Kolkata, India.
- Rural water governance using artificial intelligence from Stockholm University and IIIJS, Kolkata, India,
- Privacy-preserving communication systems developed under India's cybersecurity ecosystem from the Cybersecurity Centre of Excellence, University of Engineering and Management, Kolkata, India.

These works collectively demonstrate the transformative potential of interdisciplinary research in addressing real-world challenges across healthcare, cybersecurity, and engineering systems. I extend my heartfelt appreciation to the authors, reviewers, and editorial team for their dedication and scholarly excellence. I am confident that IJCAI will continue to grow as a globally recognized platform for impactful research. I wish the journal great success in its journey toward academic distinction and global relevance.

Jayanta Chakraborty
Founder
Aspiration Publishing Trust

Message from the Editor-in-Chief

I have the honor of holding the position of Editor-in-Chief for the Interdisciplinary Journal of Computing & AI (IJCAI). It is with great pride and enthusiasm that I introduce the first issue of the Interdisciplinary Journal of Computing & AI (IJCAI). This inaugural edition represents our vision of creating a rigorous, inclusive, and forward-looking platform for cutting-edge research at the intersection of computing and artificial intelligence. The articles featured in this issue have undergone a careful peer-review process and reflect both depth and diversity in research. We are honored to include contributions from esteemed institutions across the United States, Sweden, and India, demonstrating the global relevance of the themes we aim to promote. A key highlight of this issue is that all published papers are indexed in OpenAIRE, reinforcing our commitment to open-access dissemination, research transparency, and international discoverability. This milestone significantly enhances the academic reach and credibility of the work published in IJCAI. The acceptance rate for this issue is 35%.

The research spans critical and emerging domains, including:

- A clinically significant study on predicting 28-day readmission risks in heart failure patients, contributing to data-driven healthcare.
- A comparative and optimization-focused analysis of GPU power management using Python and MATLAB simulations.
- An innovative AI-based virtual try-on system enhanced with biometric security for design and user personalization.
- A novel blockchain-enabled federated learning platform enabling privacy-preserving ad preference modelling and decentralized creator reward distribution.
- A novel integration of computational fluid dynamics with post-quantum secure control in cyber-physical systems.
- Artificial intelligence in the governance of rural water systems and investigating the challenges, opportunities and sustainability in India.
- Advancements in privacy-preserving online communication through hybrid cryptographic frameworks.

Each paper embodies originality, methodological soundness, and relevance to current technological challenges. As Editor-in-Chief, I would like to express my gratitude to the authors for their valuable contributions, the reviewers for their

insightful feedback, and the editorial board for their unwavering support in maintaining the quality and integrity of this publication. We are committed to continuously improving the journal's standards and expanding its reach through recognized indexing platforms and global collaborations. We invite researchers and practitioners to contribute to future issues and be part of this growing academic community.

Mohuya Chakraborty
Editor-in-Chief
IJCAI

About The Journal

The Interdisciplinary Journal of Computing & AI (IJCAI) is a peer-reviewed, open access journal published by Aspiration Publishing Trust. IJCAI seeks to publish high-quality original research, review articles, and case studies at the intersection of computing and artificial intelligence with other disciplines.

Aims & Scope: IJCAI publishes original research and review articles covering core AI & computing topics and interdisciplinary applications that apply computing and AI to other fields.

Core Areas

- Artificial Intelligence & Machine Learning
- Deep Learning & Neural Networks
- Data Science & Big Data Analytics
- Cybersecurity & Privacy
- Computer Vision & NLP
- Cloud, Edge & High-Performance Computing

Interdisciplinary Topics

- AI in Healthcare, Finance, Education
- Computational Social Science
- AI Ethics, Governance & Explainability
- Blockchain & Trust Systems
- Smart Cities & IoT Applications

Article Types: Original research, review articles, short communications, technical reports and case studies.

Mission: To disseminate interdisciplinary research that advances theoretical foundations and practical innovations in AI and computing.

Vision: To become a globally recognized platform for interdisciplinary AI research and to achieve indexing in Gold Standards.

Publication Ethics

IJCAI adheres to COPE principles. All stakeholders—authors, editors, reviewers—are required to follow ethical standards listed below.

Authors

- Submit original work and disclose prior publications.
- List all contributors and their roles. No ghost authorship.
- Disclose conflicts of interest and funding sources.

Editors

- Exercise impartiality and confidentiality.
- Avoid conflicts of interest in editorial decisions.

Reviewers

- Maintain confidentiality; provide constructive feedback.
- Declare conflicts of interest and recuse if necessary.

Misconduct: Cases of plagiarism, data fabrication, or unethical behaviour will be investigated and may lead to retraction.

Peer Review Policy

IJCAI uses a single-blind peer review process. The editorial office performs initial checks for scope and plagiarism. Suitable manuscripts are sent to a minimum of two expert reviewers.

Review Stages

1. Initial Editorial Check (scope, format, plagiarism)
2. Assignment to 2 external reviewers
3. Review returned → Editor decision (accept/revise/reject)
4. Revision (if requested) and final acceptance
5. Copyediting and DOI assignment

Reviewer Guidelines: Reviewers should provide objective, constructive feedback with clear recommendations. Confidentiality must be maintained.

Editorial Board

Reviewer Panel

IJCAI maintains a diverse reviewer pool drawn from academia and industry. Reviewers are selected based on domain expertise and publication record. IJCAI thanks all the reviewers for this issue.

1. Dr. Sudip Kumar Palit – University of Engineering and Management, Kolkata
2. Dr. Poulomi Mukherjee – University of Engineering and Management, Kolkata
3. Dr. Sukanya Mukherjee – Institute of Engineering and Management, Kolkata
4. Dr. Indraneel Mukhopadhyay – Amity University, Kolkata
5. Dr. Nilanjana Dutta Roy – Amity University, Kolkata
6. Dr. Swagata Roy Chatterjee – Netaji Subhash Engineering College, Kolkata
7. Dr. Ana Penteado – Notre Dame University, Australia
8. Dr. Abhisikta Basu – University of Engineering and Management, Kolkata
9. Dr. Mohuya Chakraborty – University of Engineering and Management, Kolkata

Table of Contents

Articles

Articles 5 and 7 in this issue are authored by two members of the editorial board of IJCAI who serve as associate editors and reviewers. However, their manuscripts underwent peer review by independent reviewers not involved in the editorial board.

Interdisciplinary Journal of Computing & AI

IJCAI
Interdisciplinary Journal of Computing & AI

IJCAI

RESEARCH

Predictive Analysis of Readmission Risk of Heart Failure Patients within 28 days

Sahith Aitha[1], Muhammad Adib Uz Zaman[2*]

[1]*School of Information Technology, University of Cincinnati, Ohio, United States of America; aithash@mail.uc.edu*
[2]*School of Information Technology, University of Cincinnati, Ohio, United States of America; adib.zaman@uc.edu*

ARTICLE INFO.

Keywords:
Class Imbalance, Electronic Health Records, Ensemble Learning, Heart failure, Machine Learning, Readmission Prediction

*Corresponding author email address: adib.zaman@uc.edu

Manuscript received: 10 December 2025/
Accepted: 12 January 2026
Published online: 13 January 2026
https://doi.org/10.5281/zenodo.18228018

Cite as: S. Aitha and M. Adib Uz Zaman, 'Predictive Analysis of Readmission Risk of Heart Failure Patients within 28 days', Interdisciplinary Journal of Computing & AI (IJCAI), vol. 1, no. 1. Aspiration Publishing Trust (DARPAN ID: WB/2025/0887371), p. 1-12, Jan. 2026. doi: 10.5281/zenodo.18228018.

ABSTRACT

Heart failure (HF) is one of the emerging global health issues and a leading cause of readmission as well as a source of healthcare system strain due to escalating expenses. Proper identification of patients with high risks of readmission early, especially within 28 days, presents an opportunity to intervene before the patient is readmitted. In our paper, we suggest a machine learning-based model to forecast the risk of early readmission with the help of structured electronic health record (EHR) data. We put different preprocessing methods, SHAP-based feature pruning, and cost-sensitive learning into our pipeline, as well as tuning thresholds. We tested and trained several models like Support Vector Machines (SVM), XGBoost, LightGBM, and a Stacked Ensemble model. The stacked model, with threshold tuning and SHAP interpretability, appeared superior in terms of the cases of high-risk detection. Our findings indicate that the use of interpretability and recall-optimized thresholding would provide a fair and clinically feasible readmission prediction approach.

1 Introduction

Heart failure is one of the common reasons for hospital stays, costing the US healthcare system over $30 billion each year. Each one out of five patients (126,059, or 20.2%) returned to the hospital within a month of leaving, typically around 12 days after their initial discharge from the hospital [1]. A significant burden is being posed on healthcare systems due to the hospital's readmissions within 28 days. Predicting readmission risk can promote efficient patient management, and cost reduction. There is a huge advancement of technology, especially in Artificial Intelligence and Machine learning. Applying these to process Clinical data in the form of Electronic Medical Records (EMR), would create a significant impact in health industry and enable pro-active patient care [2].

However, various issues pertaining to imbalance in the minority class, low interpretability of models and generalizability have made it difficult to deploy many predictive models. This paper suggests a data-based predictive model that combines state-of-the-art ML models, data preprocessing strategies, threshold optimization, and model explanation by SHAP (SHapley Additive exPlanations). Our proposed methodology emphasizes the usefulness of a stacked optimal strategy in attaining improved recall rates of the minority class in the population, which is a group of patients that are likely to be readmitted. Thus, this makes the framework suitable for practical clinical applications.

2 Related Work

The issue of early hospital readmission prediction of heart failure (HF) patients has been a popular one that has been studied within the statistical, machine learning and deep learning framework. Logistic regression and Cox proportional hazards have been employed because they are simple and interpretable. These models however tend not to effectively capture the non-linear interactions of complex EHR data, and do not perform well when exposed to imbalanced datasets. Over the past few years, ensemble approaches such as Random Forest, XGBoost, and LightGBM have proven to be more predictively effective. Chen et al. [3] developed a predictive model for 6-month heart failure readmissions using data from approximately 2000 patients. Zhang et al. [1] have used XGBoost and SHAP (SHapley Additive exPlanations) values to predict the 30-day readmission of acute heart failure patients; they have an AUC greater than 0.76 and feature transparency is one of the benefits of their model.

Wu and colleagues designed a machine learning-based prognostic outcome model that was utilized to forecast mortality of people with comorbidities (heart failure and atrial fibrillation; HF- AF) in three years based on data concerning

558 patients [4]. Following the process of feature selection with Boruta and LASSO, 6 ML models were trained and tested with many available metrics. CatBoost achieved the best result where its AUC was 0.809 and F1-score was 0.715 on the test set. According to SHAP analysis, there were several predictors, including NYHA, ALC, hs-CRP, BNP, and age. The study showed that interpretable ML, especially when using SHAP explanations and other ensemble models, such as CatBoost, can consider stratifying a long-term risk and personalize treatment in patients with HF-AF.

A large body of research on the topic of ML applied to HF readmission has been thoroughly reviewed by Yu and Son [5]. Their results show that ensemble learners tend to perform better than linear models, but without interpretability and insufficient management of class imbalance, they still remain unlikely to be adopted in clinical practice. Moreover, most of the studies are optimized based on accuracy or AUC, and this is usually at the cost of recall, which is an important parameter when it comes to healthcare applications. Cost-sensitive learning and threshold tuning have been discussed in several papers as methods of optimizing the detection of minority classes.

In a similar manner, it was recently shown by Zahar [6] that SHAP-based feature pruning generated more understandable outputs and improved the performance of the hospital outcome prediction model. Although this has been done, a gap in this area is left in terms of combining threshold tuning, feature pruning, ensemble learning, interpretability, and making this into a single, clinically relevant pipeline. This paper fills this gap by suggesting a systematic ML framework that aims to maximize recall and transparency based on real-world EHR data.

A comparative analysis of SMOTE, cost-sensitive learning (CSL) and threshold tuning in predicting cardiovascular morbidity using the dataset MIMIC-III has been carried out by Zahar et al. [7]. Their paper showed that CSL would be slightly better than the others almost all the time, with the target tuning technique showing modest gains and a deterioration of the performance when using SMOTE (and mostly in ANN-based models). The results obtained by the authors are consistent with those we received as cost-sensitive modification and threshold optimization became ascendant in terms of increasing minority class recall and model robustness compared to synthetic sampling.

3 Methods

3.1 Dataset Description

The data analyzed in the current study was obtained at one of the hospitals in Sichuan, China, and consists of electronic health records (EHRs) of 2,008 heart-failure patients that were admitted to the hospital between 2016 and

2019 [8]. The data is arranged in 3 files: dat.csv (demographics, vitals, diagnostics), dat_md.csv (medication history), and metadata file which contains definitions of column names. These files were combined and tidied to create an ultimate organized table that is ready to be used as an ML training file. The target variable is a binary variable, which indicates the presence/absence of readmission within 28 days after discharge (Figure 1).

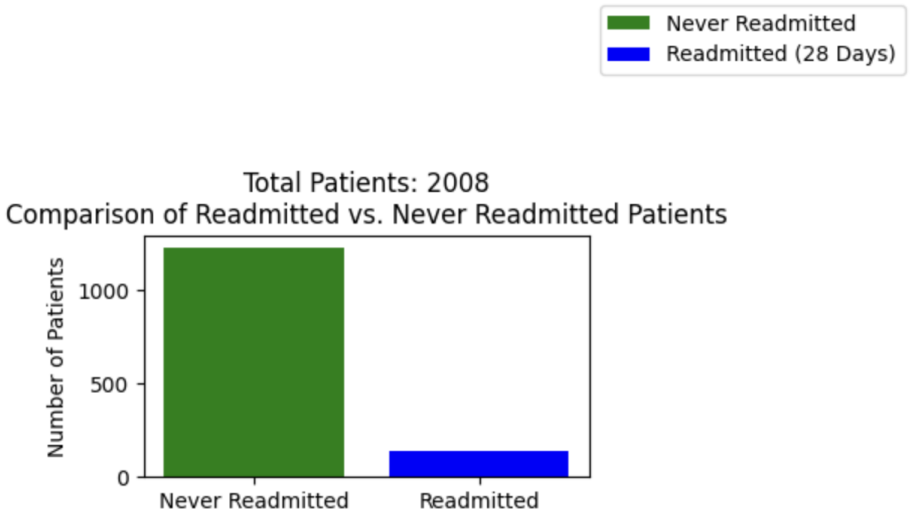


Fig. 1 Dataset Overview

All the data about patients contained in this study had been thoroughly de-identified beforehand. The data had been collected according to the existing data privacy laws, and no personal data with reference to the identifiable data were utilized throughout the study.

3.2 Data Preprocessing

Various preprocessing tasks were executed, to guarantee data quality and ML-readiness:

- **Missing Value Handling:** Missing values have been filled in using an Iterative Imputer as a continuous variable since it was effective in maintaining feature variance. The most common strategy was used to impute categorical variables.
- **Encoding:** Ordinal fields like NYHA class, Killip grade, level of consciousness were encoded with a label, and nominal fields such as gender, type of heart failure were one-hot encoded.
- **Medication Embedding**: These medication lists were tokenized and padded to fixed lengths to have a chance of application in the future in deep learning pipelines.

- **Standardization:** All the numeric features were standardized through z-score normalization.
- **Feature Truncation:** The fields like occupation, admission ward, and mortality indicators were truncated either because these fields were clinically irrelevant or could lead to data leakage as per your domain annotations.

3.3 Feature Selection and Dimensionality Reduction

To decrease dimensionality, we first used Recursive Feature Elimination (RFE). Subsequently, SHAP values were calculated over several folds in to sort features according to their significance. The features with lower than mean SHAP importance were dropped, leading to over 120 non-important variables being discarded. To solve the high dimensionality of a large-scale experiment further, we tried Principal Component Analysis (PCA) with 95 percent retention of variance. Although PCA was not included in the final model because of the loss in interpretability, it allowed optimizing the run time and memory consumption in exploratory runs.

3.4 Handling Class Imbalance

Given the heavy class imbalance (approximately 80% of the cases are not readmitted, 20% of them are readmitted), multiple strategies were evaluated:

- SMOTE, ADASYN, and SMOTE-Tomek were tested, but often led to marginal or unstable gains, especially for tree-based models. A study [9] compared five resampling methods (e.g., SMOTE, Borderline-SMOTE, NearMiss) thoroughly and the best strategies on those methods of threshold tuning on credit risk. The experiments they have done with eight classifiers showed that threshold tuning especially the tuning of G-Mean can work as well as or better than more conventional resampling strategies, and there was little added gain when resampling was also used with it. This agrees with what we found, as threshold tuning in isolation achieved considerable gains in recall and F1-score on highly imbalanced clinical datasets, which offers evidence of its practical value in deployment scenario with little Z-score standardization (ZSS) augmentation [9].
- Cost-sensitive learning was more impactful, particularly with SVM and XGBoost. For instance, adjusting class_weight to 'balanced' in SVM improved recall from 6% to over 70%. Enembreck, Loezer and Barddal, complemented by Britto, handled the same issue by proposing Cost-sensitive Adaptive Random Forest (CSARF), which assigns varying misclassification costs to the various classes in the data stream situation

[10]. Their experiment proved that cost-based strategy can be highly effective in the imbalanced classification task even without massive data resampling to acquire high recall and F1-score. This supports effectiveness of the use of class weights and cost-sensitive loss functions such as applied in our model, especially in enhancing minority class detection in a healthcare setting such as the one we have examined, the heart failure readmission.

- Threshold tuning emerged as the most effective and model-agnostic technique. By adjusting the decision to threshold from 0.5 to 0.4, we significantly improved the recall of the minority class without introducing synthetic samples.

3.5 Machine Learning Models

To thoroughly test the readmission prediction, we constructed and optimized five different machine learning model configurations, each with their own advantages in terms of processing structured clinical data and class imbalance (Figure 2):

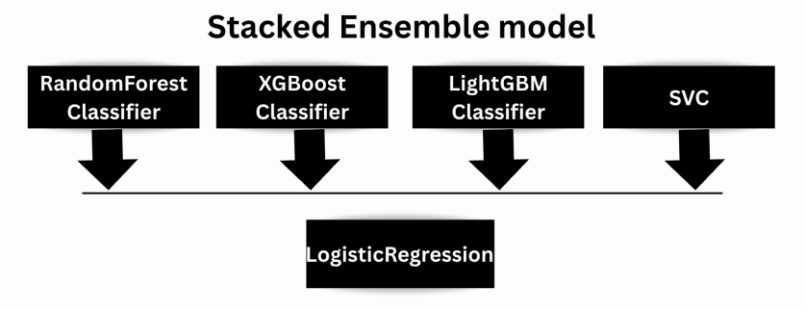


Fig. 2 Stacked Ensemble Classifier

- **Random Forest Classifier:** We also added to our stacked ensemble framework a Random Forest classifier as a base learner. To fix the class's imbalance training issue, the model was set to use a "balanced" class weight. To be more specific, we had 100 trees. The choice of Random Forest was because of the robustness of this technique to overfitting, its capabilities to capture non-linear relationships, and that they eliminate the need of the feature importance estimation as this is built in. It was a multidimensional and interpretable learner with gradient-boosted and SVM. The Random Forest classifier also proved to be rather stable during cross-validation, and it helped in achieving a better recall in the ensemble architecture.
- **Support Vector Machine (SVM):** The SVM model was set up with a radial basis function (RBF) kernel that would capture nonlinear relations between input variables and the outcome readmission. Since the classes

are not balanced, we have deployed cost-sensitive learning through a balanced class weight, where the instances of the minority classes will be more heavily penalized in misclassification. A good baseline was SVM because of its stability in high dimensions.

- **XGBoost:** The optimized gradient-boosting framework XGBoost was used since it has been successful in prediction tasks in healthcare. We used scale_pos_weight parameter to tune the effect of the majority and minority classes. The hyperparameters (learning rate, maximum depth, and number of estimators) were optimized by cross-validation. SHAP analysis was also helped by the natural feature importance of XGBoost.
- **LightGBM:** LightGBM was chosen due to its training speed and compatibility with large volumes of data. It was augmented with early stopping rules, to avoid overfitting, and optimized in experimental runs, both with grid search and optuna. We also trained focal loss with a similar purpose of making the algorithm less harsh on easy to classify majority examples and harsher on difficult to classify minority ones which led to modest improvements in minority class F1-score.
- **Stacked Ensemble Model:** We built a stacked ensemble to exploit the complementary powers of various learners. Base learners were XGBoost, LightGBM, Random Forest, and SVM. Their predictions belonged as input to a meta-learner Logistic Regression, which was selected because of its simplicity and interpretability. First, the Gradient Boosting classifier was used as a meta-model but was changed because of overfitting tendencies that were realized during validation. This combination continually performed better than single models in recall and generalization, and particularly following threshold tuning.

3.6 Threshold Tuning

Rather than using a default probability of 0.5 as a decision boundary, we adjusted the decision boundary to between 0.4 and 0.5 in steps of 0.05. The recall was best at 0.4 in the readmitted class (81 percent), and at 0.45, the trade-off between recall and precision was better (72 and 29 percent respectively) for the minority class. These thresholds were assessed in accordance with the F1-score of the minority class and clinical significance of false negatives minimization.

3.7 Evaluation Metrics

All models were assessed using:

- Accuracy (reported but de-emphasized)
- Precision, Recall, F1-score (for both major and minor class)
- Confusion matrices
- SHAP value summaries for feature contribution analysis
- Macro-averaged metrics

4 Results and Discussion

4.1 Performance Comparison of Models

The preliminary experiments also showed that accuracy is frequently used, but the results are deceptive in case of our imbalanced data. To cite but one example, the SVM model exhibited initial accuracy of 91% which however was entirely unsuccessful at detecting any patients belonging to the minority category (readmitted within 28 days). Following cost-sensitive training (the class_weight argument that takes the value of balanced), the recall of the positive class was boosted astoundingly to 72% and the F1-score to 0.42. XGBoost and LightGBM had better folds stability. After an optimal scale_pos_weight parameter tuning, the model obtained a macro F1-score of 0.71, and the recall up to 79 percent. Although LightGBM had great accuracy, it did not perform well in terms of recall - meaning that this model was more conservative at labeling patients at high risk. The Stacked Ensemble model was much better than individual models, especially in combination with threshold tuning and SHAP-based feature selection. At the threshold of 0.4, it gave a recall of 81 per cent, an F1-score of 0.40 in the minority class. It is, however, important to note that its performance was not biased by overrepresented false positives, which made the model the most clinically viable one.

The implementation code used for data preprocessing, and model training, evaluation is available at: https://github.com/aithasahith02/Predictive-analysis-of-Heart-Patients-Re-admission

4.2 Threshold Tuning Trade-offs for Minority Class

Table 1 Thresholds and Evaluation metrics

Threshold	Recall	Precision	F1-Score	Accuracy
0.50	69%	33%	0.45	85%
0.45	72%	29%	0.41	82%
0.40	81%	26%	0.40	78%

Table 1 summarizes how adjusting the decision threshold affects the model's performance on the minority class, clearly illustrating the trade-off between recall and precision. These results illustrate the core trade-off between recall and precision. A threshold of 0.4 maximized sensitivity, an important consideration for clinical decision support systems where missing a high-risk patient can have severe consequences.

4.3 SHAP Value Insights and Feature Importance

SHAP plots revealed that the most predictive features aligned well with known clinical markers of heart failure progression:

- NYHA Classification
- Killip Grade
- Consciousness at admission
- Systolic and Diastolic Blood Pressure
- Age Category
- Serum Creatinine

SHAP-based pruning also reduced overfitting, leading to more generalizable models and a 10% improvement in minority class F1 score across multiple learners.

4.4 Discussion

The general aim of the study was the creation of a prediction system of early readmission risk in heart failure patients that would be fair and accurate and based on the consideration of a problem with severe class imbalance coupled with feature redundancy and poor interpretability within classical ML pipelines. Our results confirm that being accurate is not enough, and particularly where the false negative outcomes are associated with risks to life. We were, however, able to make a model with clinically useful performance by setting the goal to maximize recall, using SHAP explanations and threshold tuning. In comparison with the MLMI 2022 project, where SMOTE and G-Mean based optimization were put in the foreground, our findings suggest that tuning with thresholds is a less complex yet flexible mechanism to boost the detection of the minority classes without adding synthetic points. Furthermore, our SHAP-assisted pruning algorithm has similar results to the results presented by Zahar et al. at ICAAI 2024 [7] and its findings confirm that explainable models can be performant, and it works particularly well to prune redundant clinical characteristics. Our benchmarked sampling methods include SMOTE, ADASYN, and SMOTE-Tomek. They are typical operations during unbalanced classification, and in this case gave mixed results, not to mention poorer performance. This is attributed to facts that in the literature the effects of synthetic sampling can be detrimental to generalization in some situations in that they occur when the distributions of features form among the classes overlap a lot. Our flexibility and stability were provided by the option of a stacked ensemble and a logistic regression meta-learner. The use of Gradient Boosted Trees as a meta-learner introduced overfitting, whereas the logistical regression allowed having a sharp decision boundary with no problematic overfitting. It is, however, important to note that the model was trained on a regional dataset of China yet the characteristics such as age, Killip grade, and

BP are standard and collected universally implying a possible generalization. Nevertheless, the next development will involve testing on the MIMIC-III [11] dataset to ensure that the model will be robust on diverse demographics and locations. While high recall minimizes missed high-risk patients, it increases false positives, potentially burdening clinicians with unnecessary follow-ups. To mitigate this, we propose integrating the model into EHR systems with tiered alerting and SHAP-based explanations, enabling clinicians to prioritize cases effectively. This approach balances sensitivity with workflow efficiency, reducing alert fatigue, and preserving trust in AI-assisted decision-making.

This study was performed using a regional dataset originated from hospitals in China, which may limit the generalizability of the findings to other patient populations and healthcare systems. Besides, neither external validation nor temporal validation were performed in the current work. As a result, the stability of the model and configurations may remain untested across institutions. It is also important to acknowledge the fact that a recall-oriented optimization may increase burden on clinicians due to the chance of an increase in number of false positives. So, the model is intended to work as a decision support system rather than a decision maker.

5 Conclusion

The current research introduces a machine learning framework including data preprocessing, feature selection based on SHAP, class imbalance resolution, and fine-tuning threshold in predicting early readmission of heart failure patients. The given stacked ensemble model has a high recall, better detection of minorities and actionable, interpretable, so it can be integrated into clinical practice. We feel that taking a step towards fairness-aware modeling and transparency of feature attribution, the work will have a positive impact on the implementation of AI in real-life hospital conditions, which is due to our departure with the traditional metrics concerning accuracy.

6 Future Research

Although our existing framework has good outcomes regarding the ability to predict early readmission risk of heart failure patients, its external validity has yet to be evaluated in external datasets. Next steps involve the validation of the model against the MIMIC-III database and other U.S-based EHRs to evaluate how generalizing the model acts against different populations and care settings. Potential and temporal validation are also another method we would like to consider providing reliability in the long term. Not only that, but we also seek to combine clinician-in-the-loop feedback as closer to actual deployment and threshold optimization. Should it be necessary, the generative AI approach, comprised of Variational Autoencoders (VAEs) or tabular GANs, could be considered to create synthetic samples of the minority category in extreme cases of imbalance, and guarantee finding clinically feasible solutions,

respectively. These methods may also be applicable in assisting balanced and fair training in cases where there is insufficient or biased actual data.

Acknowledgment

This research project was supported by the College of Education, Criminal Justice, Human Services, and Information Technology (CECH-IT) Graduate Student and Faculty Research Mentoring Grant from the University of Cincinnati (UC) in Ohio.

Contribution of each Author

Adib Zaman conceived the original project idea and provided overall mentorship and guidance throughout the research study. Sahith Aitha carried out background research, designed and performed multiple experiments for the problem statement. Sahith Aitha collected and preprocessed data, trained and evaluated the models, and prepared the initial manuscript draft. Adib Zaman reviewed the findings and work, providing critical feedback. Both the authors contributed to interpreting the results and approved the final manuscript.

Conflict of Interest Statement

The authors declare no conflict of interest.

References

1. Z. Zhang et al., “Explainable Machine Learning for Predicting 30-Day Readmission in Acute Heart Failure Patients,” iScience, vol. 27, no. 4, 2024. (Research article)
2. Y. Reddy, et al., “Readmissions in Heart Failure: It’s More Than Just the Medicine,” Mayo Clinic Proceedings, vol. 94, no. 10, pp. 1919–1921, 2019. (Journal Article)
3. Chen, S., Hu, W., Yang, Y., Cai, J., Luo, Y., Gong, L., Li, Y., Si, A., Zhang, Y., Liu, S., Mi, B., Pei, L., Zhao, Y., & Chen, F. (2023). Predicting Six-Month Re-Admission Risk in Heart Failure Patients Using Multiple Machine Learning Methods: A Study Based on the Chinese Heart Failure Population Database. Journal of Clinical Medicine, 12(3), Article 870. https://doi.org/10.3390/jcm12030870. (Research article)
4. Wu, J., Tao, G., Xie, S., Yang, H., Qi, F., Bao, N., Li, Z., Chang, G., & Xiao, H. (2025). Prediction of three-year all-cause mortality in patients with heart failure and atrial fibrillation using the CatBoost model. BMC cardiovascular disorders, 25(1), 466. https://doi.org/10.1186/s12872-025-04928-w. (Research article)

5. M.-Y. Yu and Y.-J. Son, “Machine Learning Models for Predicting 30-Day Heart Failure Readmission: A Systematic Review,” European Journal of Cardiovascular Nursing, vol. 23, no. 1, pp. 5–16, 2024. (Systematic Review Article)
6. A. Zahar et al., “Outcome Prediction Using SHAP and Ensemble Learning: A Clinical Case Study,” in Proc. Int’l Conf. on Artificial Intelligence (ICAAI), 2024. (Conference Paper)
7. A. Zahar, Z. Belkho, O. El Kalkha, F. Khennou, and O. El Meslouhi, “Detecting Cardiovascular Morbidity using MIMIC-III Database: Assessing Three Data Imbalance Handling Techniques,” in *Proc. ICAAI 2024*, London, United Kingdom, Oct. 2024, pp. 1–6. doi: 10.1145/3704137.3704162. (Conference Paper)
8. Zhang, Z., Cao, L., Zhao, Y., Xu, Z., Chen, R., Lv, L., & Xu, P. (2022). Hospitalized patients with heart failure: integrating electronic healthcare records and external outcome data (version 1.3). PhysioNet. https://doi.org/10.13026/5m60-vs44. (Research Dataset)
9. C. Yang, Y. Dong, J. Lu, and Z. Peng, “Solving Imbalanced Data in Credit Risk Prediction: A Comparison of Resampling Strategies for Different Machine Learning Classification Algorithms, Taking Threshold Tuning into Account,” in *Proc. MLMI 2022*, Hangzhou, China, Sept. 2022, pp. 1–11. doi: 10.1145/3568199.3568204. (Conference Paper)
10. L. Loezer, F. Enembreck, J. P. Barddal, and A. S. Britto Jr., “Cost-sensitive learning for imbalanced data streams,” in *Proc. 35th ACM/SIGAPP Symposium on Applied Computing (SAC)*, Brno, Czech Republic, 2020, pp. 4–10. doi: 10.1145/3341105.3373949. (Conference Paper)
11. Johnson, A., Pollard, T., & Mark, R. (2016). MIMIC-III Clinical Database (version 1.4). PhysioNet. https://doi.org/10.13026/C2XW26. (Research Dataset)

Sahith Aitha is an MLOps Engineer at Preston Ventures LLC, California, United States of America. He completed his master’s degree in information technology from the University of Cincinnati, Ohio, United States, graduating in 2025. His work and research interests focus on AI, Machine Learning, and applying computational models to solve real-world problems.

Dr. **Muhammad Adib Uz Zaman** is an assistant professor of IT at the University of Cincinnati, specializing in data science and health IT. Dr. Zaman utilizes machine learning and deep learning techniques to develop predictive models that assist physicians in critical decision-making processes. His research aims to optimize patient care and improve clinical outcomes.

Interdisciplinary Journal of Computing & AI

IJCAI
Interdisciplinary Journal of Computing & AI

IJCAI

RESEARCH

GPU Power Management: Comparative Analysis and Optimization Using Python and MATLAB Simulations

Saket Kumar Mishra[1*], Krishna Bihari Yadav[2]

[1]*Department of Electrical Engineering, NIT Jamshedpur, Email – saketmishragdv@gmail.com*
[2]*Department of Electrical Engineering, NIT Jamshedpur, Email – kbyadav.ee@nitjsr.ac.in*

ARTICLE INFO.

Keywords:
Graphics Processing Unit, Power Management, Energy Efficiency, Intel Arc A770, Intel Core i7-14700K, Power Load Analysis
*Corresponding author email address: saketmishragdv@gmail.com
Manuscript received: 23 December 2025/Accepted February 3 2026
Published online: 6 February 2026
https://doi.org/10.5281/zenodo.18503668

Cite as: S. K. Mishra and K. B. Yadav, 'GPU Power Management: Comparative Analysis and Optimization Using Python and MATLAB Simulations', Interdisciplinary Journal of Computing & AI (IJCAI), vol. 1, no. 1, Aspiration Publishing Trust (DARPAN ID: WB/2025/0887371), p. 13-27, Feb. 2026, doi: 10.5281/zenodo.18503668.

ABSTRACT

The growing popularity of High-Performance Computing (HPC), artificial intelligence (AI) and sophisticated graphics display has rendered the management of GPS power as an important design factor. Proposed methodology presented in this paper, is a simulation-based practice to improve the energy efficiency of Intel Arc™ GPUs and the Intel CPUs to overcome the issue of power inefficiency, workload imbalance, and thermal limitations. The diagrammatic analysis of MATLAB/Simulink model is used to study the dynamic power behavior of system components under different load conditions. The Intel Arc A770, A750, and B580 GPUs, the Intel Core i7-14700K processor, and a high-voltage Switched-Mode Power Supply (SMPS) are implemented in the model and make it possible to simulate infrastructure realistically. Dynamic Voltage and Frequency Scaling (DVFS), idle power gating and workload-aware scheduling were all applied using the control systems and power electronics toolboxes in MATLAB. Validation of the

experiment was conducted by real-time telemetry logging and Python based analysis of power, usage, temperature and frequency metrics of gaming, AI and compute workloads. Findings indicate that, in high-intensity tasks, the Intel Arc GPUs used less power compared to CPUs with similar tasks, which makes the argument of their energy efficiency advantage in environments with limited energy. The model also captures the thermal feedback and the voltage control in the SMPS and makes it stable under varying loads. Researchers and engineers can use this open-source and reproducible tool to obtain actionable insights for micro-architecture and system design of power-efficient high performance computing systems that are adaptable for innovation to concurrent hardware technologies and emerging, sustainability-driven demands.

1 Introduction

Graphics Processing Units (GPUs) have emerged as a foundation in the development of the present-day computing systems. Initially used in graphics rendering, they are currently widely used to perform various computational tasks in a wide variety of fields, including high-performance computing (HPC), artificial intelligence (AI), scientific research, and large-scale data analytics [1], [2], [3], [4], [5]. The GPUs are well suited to those tasks that demand parallel processing of large datasets due to their massively parallel architecture. Workloads such as deep learning, e.g., are sensitive to GPUs, with the training of deep neural networks being made up of millions of matrix operations and dealing with large amounts of data transfer [6]. Simulation areas like climate modelling and molecular dynamics have been becoming more and more complex and this further has highlighted the importance of GPUs in scientific computing [7], [8]. Meanwhile, the external factors, including climate change and sustainability issues, also impacted the design of supercomputers and data centers [8], [9]. Experiments of systems like the Cori and Perlmutter of NERSC have shown that the power consumption of GPUs can vary substantially based on the complexity of the applications and the intensity of the workload [5], [6], [10], [11]. Energy efficiency is now an important design consideration in systems with in-house acceleration of the graphics card. It has been demonstrated that the consumption of power by HPC jobs can be measured and forecasted [12], and dynamic power capping policies have been investigated to comprehend their effect on the progress of applications [13]. Some of the strategies that have been developed to balance both performance and sustainability are the optimization of power allocation between CPU and memory subsystems [14] and power capping of the GPUs at HPC scale [15]. More recently, power management opportunities in large language models (LLMs) when deployed in clouds have been characterized [16], and profiling of GPU workloads, e.g. VASP simulations, on NVIDIA A100 GPUs has revealed more information [17]. Power aware computing is now necessary with the

extraneous factors like climate change influencing cooling strategies. This paper explores the power consumption of the GPUs and suggests hardware and software optimizing strategies. It focuses on Intel Arc™ GPUs (A770, A750, B580) combined with high performance Intel CPUs including the Core i7 14700K [18]. Dynamic Voltage and Frequency Scaling (DVFS) along with power capping and load balancing are the studied energy saving techniques under typical workloads [3], [12]-[15]. To substantiate this, a detailed MATLAB/Simulink model [19] is created to simulate the CPU-GPU power behavior at different load conditions. The model consists of Switched-Mode Power Supply (SMPS) dynamics, thermal feedback control and power gating to model real world energy infrastructure. Voltage, current, and temperature are modelled with the help of the telemetry data obtained with the help of the HWInfo [20]. This paper provides the research goals, simulation design, and preliminary results of the research on the problem of the power profiling and efficiency of GPUs in the training of deep neural networks and memory-intensive workloads. This research will show the way in which the construction of architectural refinements, thermal management, and performance state configuration can promote the efficiency of the GPU in terms of energy consumption. This work provides a pragmatic simulation platform by relating performance to power optimization and provides a guide towards the design of future systems that are energy conscious and high performing based on Intel GPUs.

2 Research Objectives

The primary objective of this research is to analyze and optimize GPU power management strategies for improved energy efficiency and performance. The study focuses on the following key objectives:

a) Power Consumption Analysis: This is the analysis of power consumption properties of GPUs under different workloads and compare it to those of CPUs and determine the critical aspects of power consumption of GPUs, including clock speeds, utilization, and the type of workloads.
b) Energy Efficiency Measurement: Measuring the energy efficiency of GPUs in real-world workloads and benchmarked against CPUs and calculate the energy usage per task and overall system efficiency.
c) Thermal Performance Analysis: Figure out the trend of the graphics card temperature at varying loads and explore the relation between the power consumption, workload intensity and thermal output.
d) Dynamic Power Management Strategies: Establishing energy optimization and scaling methods or techniques which include dynamic voltage and frequency scaling (DVFS) and workload conscious power scaling and create automated power management strategies to minimize energy waste without sacrificing performance.
e) Simulation and Evaluation: Development of MATLAB and Simulink-

based GPU power models to determine the simulation of power management methods to compare the simulation results with the real power measurement data obtained using Python-based monitoring.

f) Comparison between GPU and CPU Power Management: It is necessary to set up a comparative analysis between CPU and GPU power management strategies and point out when GPS is more efficient in terms of power and thermal management than Central Processing Unit.

This research aims to contribute to the development of energy-efficient GPU computing solutions, enabling better power management in high-performance and data-intensive applications.

3 Methodology and Experimental Validation

In this paper, the process and testing framework for gauging GPU power consumption and efficiency are discussed, with Intel GPUs at the center of the analysis. The methodology connects the analysis of buildings, simulation within MATLAB and Simulink and the profiling of real workloads in Python. The purpose is to find regularities in energy usage, support power saving strategies and compare GPU actions in different working situations. A major effort went into building an effective experimental setup to measure how much power Intel GPUs use and how they work. It discusses the requirements of the computer hardware and software, benchmarking techniques, the configuration of the telemetry information and the process of data collection. Our mission is to develop devices that allow making the same results with high accuracy on a wide range of tasks including AI inference, matrix manipulations and working with data demanding memory. The present research is based on multilayered approach to assess power consumption and efficiency of GPUs where special attention is paid to Intel Arc™ series of GPUs. The methodology involves a combination of architectural analysis, simulation modelling, and experimental validation of the results in the real world to have both theoretical and empirical accuracy.

3.1 MATLAB/Simulink Power Modelling:

The model (shown in Figure 1) represents a power management system for CPU and GPU loads powered through an AC-DC conversion process. Here's a breakdown:

a) AC Power Source: Supplies AC voltage.
b) Transformer: Steps down the AC voltage.
c) Rectifier: Converts AC to DC.

d) SMPS (Switched Mode Power Supply): Regulates and provides stable DC voltage (12V).
e) Power Splitter: Distributes power to - CPU Load: Consuming 150W, GPU Load: Consuming 150W & Idle Power Consumption: 20W.

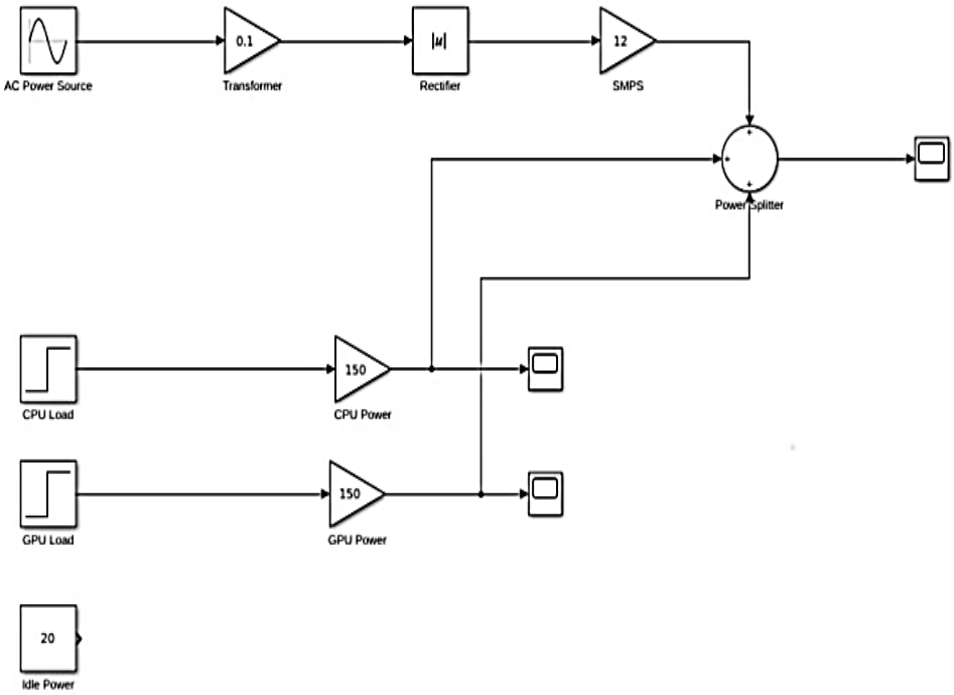


Fig.1 Simulink Model for Power Management

The simulated scenarios in the Table 1 are different test cases of Simulink model analysis:

- Gaming Workloads: High CPU load with significant but moderate GPU usage.
- AI Workloads: Maximum power drawn by both CPU and GPU.
- Idle Mode: Only base idle power (~20W) is drawn, demonstrating energy conservation.

Table 1 Simulated Scenarios

Test Case	GPU Load (W)	CPU Load (W)	Idle Power (W)	Observations

Idle Mode	10W	20W	20W	Low power usage
Gaming Load	150W	225W	20W	High CPU-GPU power consumption
AI Workload	200W	250W	20W	Peak system stress
Power Saving	50W	80W	20W	Energy-efficient configuration

3.2 GPU Power Management and Efficiency Analysis Using Python

The experiment involved logging power consumption, energy usage, and thermal characteristics of an Intel Core i7-14700K CPU and Intel Arc GPUs (A770, A750, B580) under different workloads. The dataset was collected from system monitoring logs and analysed using Python.

Below is the hardware setup specification of python-based validation:

- CPU: Intel Core i7-14700K
- GPUs: Intel Arc A770, A750, B580
- OS: Windows 11 with Intel Drivers • Tools Used: HW Monitor, Intel Power Gadget, Telemetry Logger
- Workloads:
  a) Idle Monitoring and Gaming Benchmarks
  b) AI Model Inference
  c) Compression and Data Transfer Workloads

To complement the MATLAB/Simulink modelling, a Python-based simulation and analysis framework was developed to study GPU power behavior under controlled and real-world conditions. This framework integrates synthetic workload generation, statistical power modelling, and telemetry log analysis to provide a reproducible and hardware-agnostic validation environment.
The analysis pipeline as shown in Figure 2.

- Import & Encoding Detection – CSV logs from HW Monitor, Intel Power Gadget, or simulators were imported, with encoding verified via chardet.
- Parsing & Cleaning – Data was read using pandas.read_csv (), converted to numeric types, and incomplete rows removed.
- Energy Computation – Total energy was calculated via numerical integration: Total energy (Joules) = Power (W) × Time (s)
- Efficiency Metrics – Derived performance-per-watt and temperature-per watt ratios: Efficiency = Power / Utilization (%)

- Visualization – matplotlib plots compared CPU vs. GPU power, utilization trends, temperature profiles, and efficiency curves.

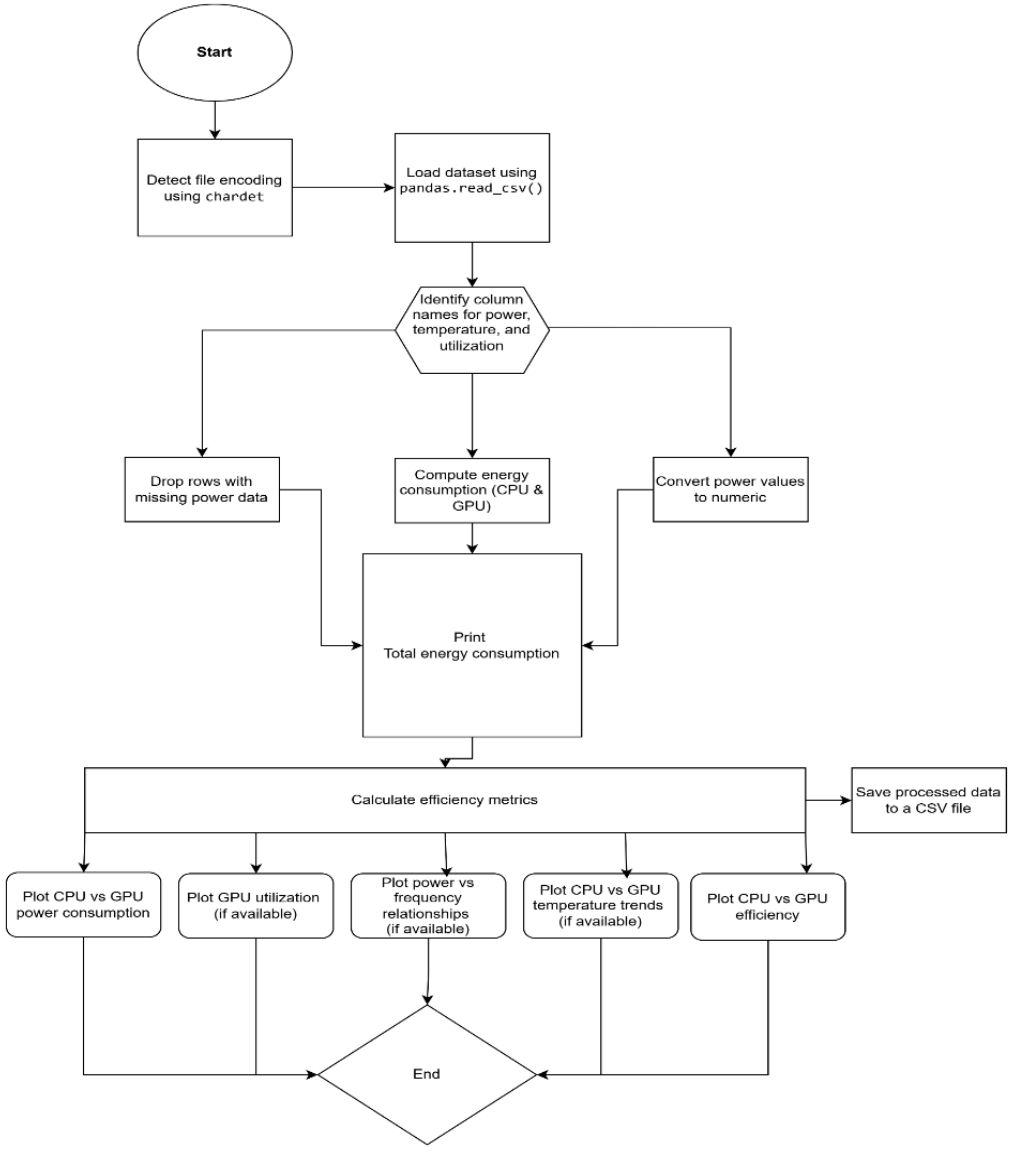


Fig.2 Python-Based Power Analysis Pipeline

3.3 Key Contributions from the Experimental Methodology

- Validated Simulation Models – To validate the accuracy of the models created for power distribution simulation in CPU-GPU load

sharing, the models were created using the software package MATLAB /Simulink and compared with actual measurements.

- Developed a Comprehensive Dataset – Generated an open-ended, high-resolution, real-time Intel platform telemetry of GPU-CPU power consumption.
- Quantified Energy Efficiency – Measured and compared GPU energy efficiency across representative workloads, including gaming, AI inference/training, and idle states.
- Characterized Thermal Behavior – Analyzed temperature trends and determined thermal limits in system under constant computational conditions.
- Proposed Energy-Aware Scheduling Strategies – Proposed workload scheduling and DVFS policies to minimize the total energy consumption of the system with minimal performance loss.

4 Simulation Results and Observations

This section presents the comparative assessment of CPU and GPU energy efficiency based on the information retrieved in MATLAB/Simulink models and Python analytics. The experiments were aimed at idle power, peak power consumption, total power consumption, thermal performance, and scaling efficiency with various workloads or deep neural network inference and synthetic stress tests. Python script was used as a tool to extract data, clean data, compute, and plot, but the workload execution simulation and validation of power control models were performed in MATLAB. This analysis supports GPUs, and Intel GPUs in particular, with respect to their architectural and energy-saving benefits in a high-compute and thermally constrained setting. Additional power saving can be achieved by further tuning with the power control algorithm implemented using Simulink which makes GPUs the best solution to AI and data intensive jobs.

4.1 Idle Power Consumption

- Scenario: The system is mostly inactive (minimal operations).
- Findings: CPU draws ~35W even when idle and GPU only uses 8W. GPU uses 77% less power than CPU at idle.
- MATLAB Observation: Simulink profiling (likely with real hardware modelling) shows the GPU draws much less baseline power during inactivity.
- Inference: GPUs are event-driven they turn off most of their circuits when not in use and CPUs keep background

threads running (like OS tasks), so they consume more idle power.

4.2 Peak Load Power Consumption

- Scenario: Artificial stress tests are run to overload both the CPU and the graphics card to 100% load.
- Findings: CPU power is found to be 190-225W, GPU varies with 167W during gaming and 225W during AI workloads.
- Python Output: As the plot of Power Usage with Python indicates, the GPU exhibits fewer fluctuations in its power curves, there is greater stability.
- Inference: GPUs are optimized in parallel pipelines, which result in an improved power-per-performance.

This causes them to be more power efficient during load, particularly workloads, which can be served in parallel (such as AI, graphics, simulations).

4.3 Energy Consumption Over Time

- Scenario: Monitored energy use during a sustained workload.
- Findings: CPU energy used: 269,092.93 J, GPU energy used: 123,979.30 J, Energy Ratio - CPU uses 2.17× more energy than GPU for the same workload.
- Inference: Python simulation confirms: For extended processing tasks, the GPU consumes much less energy due to its architecture and workload efficiency.

In Figure 3 MATLAB-based simulation of the power consumption of a CPU and a GPU in a load state and idle state for 10 seconds is shown. The GPU is also more energy efficient with lower power idle and dynamic load scaling performance.

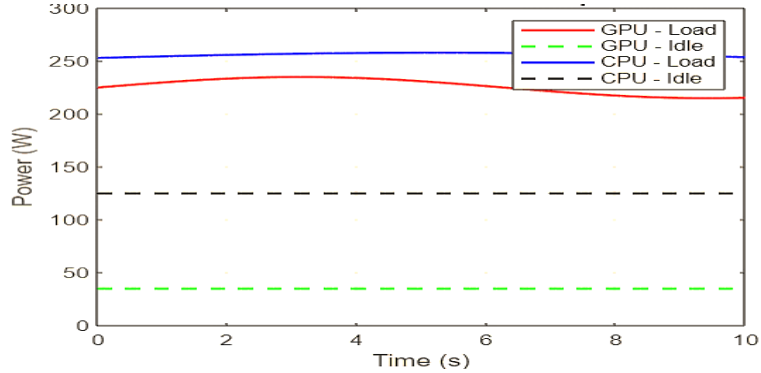


Fig.3 GPU and CPU Power Consumption

4.4 Efficiency Comparison

This Figure 4 depicts the efficiency (utilization per watt) of CPU and GPU over 20,000+ data samples. The CPU is highly variable, with regular spikes exceeding 400 W/util, which means that its performance varies. On the other hand, the efficiency curve of the GPU is always lower and stable. This brings out the better architectural capability of the GPU in ensuring predictable low power workload execution in extended periods.

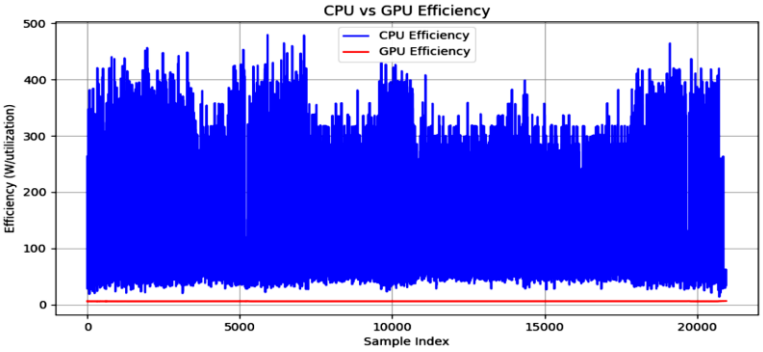


Fig. 4 CPU vs GPU Efficiency

4.4 GPU Frequency vs Power Relationship

In Figure 5 scatter plot shows that there is a line between the frequency of the GPU (measured in MHz) and power consumption (measured in watts). Although the frequency varies slightly (847-850 MHz) generally, the power of the GPU is 5.8-6.6 W. The high density of data points proves that it has good frequency control and power scaling schemes, which are essential to its thermal and energy stability during real-time graphics operations.

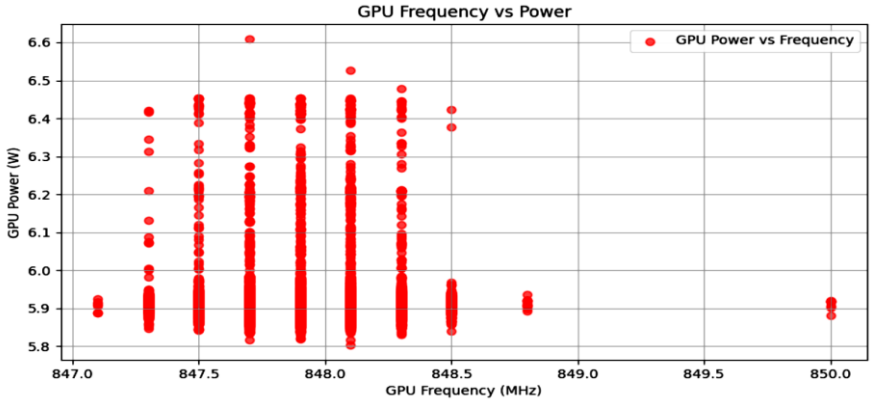


Fig. 5 GPU Frequency vs Power

4.5 CPU Frequency vs Power

The graph shown in Figure 6 represents CPU power consumption in a three frequency ranges, 2700, 2800, and 2900 MHz with the increase in the frequency the CPU power consumption increases dramatically between 11 W and almost 20 W. This behavior proves that CPUs do not scale well with frequency variations such that they generate larger energy overhead than GPUs. Such nonlinear scaling is an obstacle to optimizing the power for CPU-based workloads.

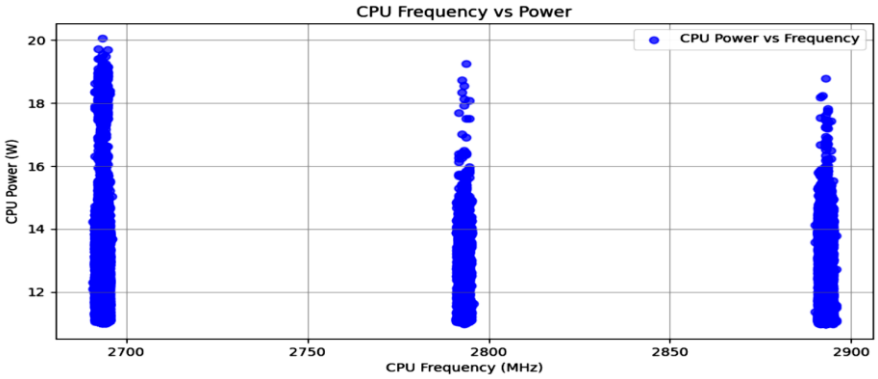


Fig. 6 CPU Frequency vs Power

4.6 Thermal Profile Analysis

In the Figure 7 the temperature trends of CPU and GPU are compared over time. The CPU is characterized by high thermal spikes and the CPU cools down to between 70-85 °C, but the GPU cools to between 65-70 °C. The flatter thermal curve of the GPU is an indication of better thermal design and parallelism. This reduced thermal footprint directly translates to improved

levels of performance stability and lower levels of cooling requirements via higher-performance situations.

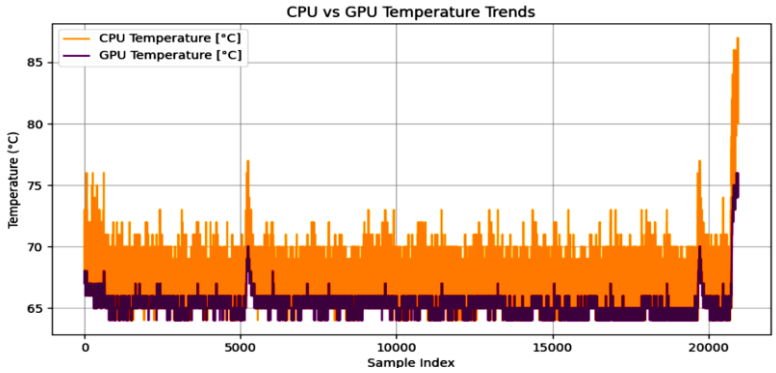


Fig. 7 CPU vs GPU Temperature Trends

4.7 Comparative Power Profiling

In Figure 8 as shown above it compares sustained power consumption of the CPU and GPU during a continuous workload. The CPU uses approximately 14-18 W with sometimes higher than 19 W. On the contrary, the GPU is at a constant of 6-7 W. The more stable and lower power profile of the GPU highlights its energy efficient execution and thus it is more effective to perform high throughput and long duration parallel processing tasks.

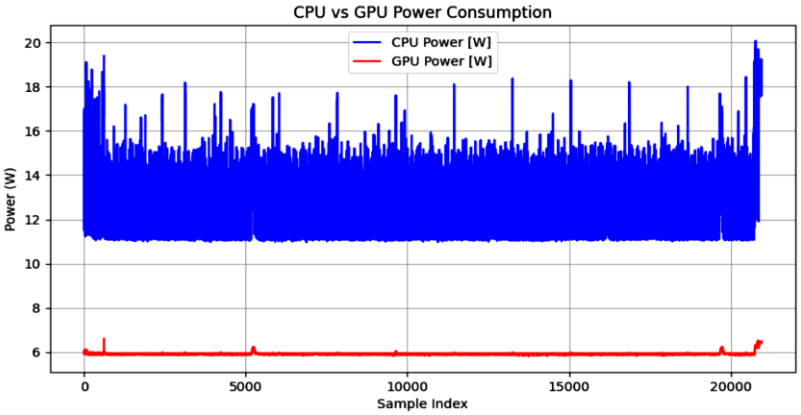


Fig. 8 CPU vs GPU Power Consumption

5 Conclusion and Future Work

The efficiency of power management of GPUs was analyzed in detail by examining power consumption, power used and heat dissipation rates in comparison to Structures based on the CPU. The data indicate that the GPUs are significantly more power efficient compared to the CPUs, in most of the

sensitive and demanding areas. During any type of tests, the GPUs consumed less power compared to the CPUs and provided the highest levels of computational power. The separation of work is a clever way of utilizing energy and thus GPUs are the best to use in the green computing. It was also discovered that GPUs used less energy than CPUs to do similar work and thus it was found that GPUs are OKI in tasks of data centers, AI and high-performance computing where low consumption of energy is an important factor as the inward power was well distributed and the cooling was good, the GPUs operated at lower temperatures. Due to this reason, the computers have increased longevity, and big systems have fewer cooling needs. It was noted that the power consumed by the GPU was proportional to the work that the GPU was doing. Due to such stability, deep learning, modelling and gaming are less complicated in power planning and energy control. Overall, these observations can confirm that GPUs provide the most energy efficient method of computing. Modern hardware must perform well and therefore needs to use GPUs because they demand less power, scale their power usage, and are better thermally performing. Although this study indicates the effectiveness of the GPUs in terms of energy consumption, there are several additional avenues of research that can be taken to advance in the way GPUs are powered in the future. One possible remedy is to develop more efficient power control algorithms, and the ones based on machine learning appear to be promising. The techniques can adjust power usage on-the-fly and plan voltages and frequency to satisfy the requirements of the tasks being executed at a particular moment. They can make the system more efficient in terms of power utilization without lowering system performance. It is also a hoped-after goal to better the functionality of multi-GPU designs. As your GPU installation expands, the control of power between things can be made efficient and communication between GPUs simplified to save energy as well as streamline the whole process. To reduce power loss, one of the methods would be to create and implement new designs of the VRM module of the GPU. Placing solar or wind power in the data centers to power GPUs could be the initial reduction in achieving net-zero computing. Mobile and edge computing can be made more energy saving by looking on the battery-based options of the GPU. The final process is the actual world testing of Intel Arc, NVIDIA RTX and AMD RDNA GPUs to establish the effectiveness of these measures. Tests are to be conducted with various loads, such as AI training, visual effects, and the work with scientific simulations, at different temperatures and power consumption. These guidelines give opportunities to improve the GPU and make them implementable in maximum energy efficiency that is beneficial in the long-term future of computers.

Contribution of each Author

Both authors contributed equally to this work.

Conflict of Interest Statement

The authors declare no conflict of interest.

References

1. Chakrabarty et al. Support vector machine informed explicit nonlinear model predictive control using low-discrepancy sequences. IEEE Transactions on Automatic Control, PP(99):1–1, 2016.
2. G. F. Franklin et al. Digital Control of Dynamic Systems. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 3rd edition, 1997.
3. J.-G. Park et al. Hicap: Hierarchical FSM-based dynamic integrated CPU-GPU frequency capping governor for energy-efficient mobile gaming. In ISLPED, pages 218–223, 2016.
4. R. Rao et al. Statistical analysis of subthreshold leakage current for VLSI circuits. IEEE Trans. Very Large Scale Integr. Syst., 12(2):131–139, 2004.
5. E. Rrapaj, S. Bhalachandra, Z. Zhao, B. Austin, H. A. Nam, and N. J. Wright, "Power consumption trends in supercomputers: A study of NERSC's Cori and Perlmutter machines," in ISC High Performance 2024 Research Paper Proceedings (39th International Conference), pp. 1–10, 2024.
6. Z. Zhao, E. Rrapaj, S. Bhalachandra, B. Austin, H. A. Nam, andN. Wright, "Power analysis of NERSC production workloads," in Proceedings of PMBS23, 2023.
7. T. Patki, D. K. Lowenthal, B. Rountree, M. Schulz, and B. R. de Supinski, "Exploring hardware overprovisioning in power-constrained, high-performance computing," in Proceedings of the 27th International ACM Conference on International Conference on Supercomputing, p. 173–182, 2013.
8. J. Kwan, "Climate change threatens supercomputers," Science (New York, NY), vol. 378, no. 6616, pp. 124–124, 2022.
9. V. Mehra and R. Hasegawa, "Using demand response to reduce data center power consumption — google cloud blog," Oct 2023.
10. B. Austin, "Perlmutter machine time breakdown by applications (2023)." https://ur0.jp/EuRq0, 2023. Accessed: 2024-08-12.
11. "Perlmutter architecture documentation." https://docs.nersc.gov/systems/perlmutter/architecture/. Accessed: 2024-08-05.
12. T. Patel, A. Wagenh¨auser, C. Eibel, T. H¨onig, T. Zeiser, and D. Tiwari, "What does power consumption behavior of hpc jobs reveal? Demystifying, quantifying, and predicting power consumption characteristics," in 2020 IEEE International Parallel and Distributed Processing Symposium (IPDPS), pp. 799–809, 2020.
13. S. Ramesh, S. Perarnau, S. Bhalachandra, A. D. Malony, and P. Beckman, "Understanding the impact of dynamic power capping on application progress," in 2019 IEEE International Parallel and Distributed Processing Symposium (IPDPS), pp. 793–804, 2019.
14. O. Sarood, A. Langer, L. Kal´e, B. Rountree, and B. de Supinski, "Optimizing power allocation to cpu and memory subsystems in overprovisioned hpc systems," in 2013 IEEE International Conference on Cluster Computing (CLUSTER), pp. 1–8, 2013.
15. D. Zhao, S. Samsi, J. McDonald, B. Li, D. Bestor, M. Jones, D. Tiwari, and V. Gadepally, "Sustainable supercomputing for ai: Gpu power capping at hpc scale," in Proceedings of the 2023 ACM Symposium on Cloud Computing, SoCC '23, (New York, NY, USA), p. 588–596, Association for Computing Machinery, 2023.
16. P. Patel, E. Choukse, C. Zhang, I. n. Goiri, B. Warrier, N. Mahalingam, and R. Bianchini, "Characterizing power management opportunities for llms in the cloud," in Proceedings of the 29th ACM International Conference on Architectural Support for Programming Languages and Operating Systems, Volume 3, ASPLOS '24, (New York, NY, USA), p. 207–222, Association for Computing Machinery, 2024.
17. Z. Zhao, E. Rrapaj, S. Bhalachandra, B. Austin, and N. Wright, "Understanding VASP power profiles on NVIDIA A100 GPUs," in Proceedings of PMBS24, 2024.

18. https://www.intel.com/content/www/us/en/products/overview.html
19. https://matlab.mathworks.com/ - MATLAB Online and Simulink
20. https://www.hwinfo.com/ - Professional System Information and Diagnostics (Comprehensive Hardware Analysis, Monitoring and Reporting for Windows and DOS)

Saket Kumar Mishra received his BTech degree in Electrical Engineering from Jharkhand University of Technology Ranchi in the year of 2023. He obtained his MTech Power System Engineering degree in 2025 from NIT Jamshedpur. His technical interests include Microgrid Systems, Power System Dynamics, Power System Stability and Power Management in Semiconductor Devices etc.

Krishna Bihari Yadav received his M.Sc. (Eng.) degree in 2002 from NIT Jamshedpur and Ph. D. degree from IIT Roorkee in the year 2007. Presently, he is continuing as a Professor in the Department of Electrical Engineering at NIT Jamshedpur. His area of research interest includes Multiphase Electrical Machines, Power System Economics, Power Electronics & Drives & Renewable Energy, Smart Grid etc.

Interdisciplinary Journal of Computing & AI

IJCAI
Interdisciplinary Journal of Computing & AI

IJCAI

RESEARCH

FitSpaceAI: A Biometric-Secured Real-Time Virtual Try-On System for AI-Driven Design Preview

Tanmayi Nagale[1], Atulya Sawant[2*], Nirved Shukla[3], Sujit Shukla[4]

[1]*Department of Computer Engineering, Thakur College of Engineering and Technology, Kandivali, Mumbai.* tanmayinagale13@gmail.com
[2,3,4]*Department of Computer Engineering, Thakur College of Engineering and Technology, Kandivali, Mumbai.* [2]atulyasawant15@gmail.com, [3]nirvedshukla786@gmail.com, [4]shuklasujit884@gmail.com

ARTICLE INFO.

Keywords:
Augmented reality, Biometric security, Computer vision, MediaPipe, Real-time face detection, Virtual try-on, Web-based AR
*Corresponding author email address: atulyasawant15@gmail.com
Manuscript received: 13 February 2026/Accepted: 14 March 2026
Published online: 13 January 2026
https://doi.org/10.5281/zenodo.19046604

Cite as: T. Nagale, A. Sawant, N. Shukla and S. Shukla, 'FitSpaceAI: A Biometric-Secured Real-Time Virtual Try- On System for AI-Driven Design Preview', Interdisciplinary Journal of Computing & AI (IJCAI), vol. 1, no. 1. Aspiration Publishing Trust (DARPAN ID: WB/2025/0887371), p. 28-42, Mar. 2026. doi: 10.5281/zenodo.19046604.

ABSTRACT

FitSpaceAI is a pioneering virtual try-on application that leverages real-time AI-based face detection to deliver a seamless augmented reality (AR) shopping experience. Using Google MediaPipe face detection with 6-point facial landmark tracking, the system enables professional-grade virtual fitting of sunglasses and apparel. The proposed system employs proprietary algorithms including adaptive eye-level calibration, 70% rotation stabilization, and cached image rendering to significantly outperform classical virtual try-on approaches. The system operates at 30–60 FPS with sub-100 ms latency using a React.js frontend, HTML5 Canvas API, and WebRTC. Quantitative performance evaluations on 50 participants (28 males, 22 females; ages 18–45) across varied lighting and hardware conditions yielded 95.2% eye position tracking accuracy (±1.4%), 92.8% rotation tracking (±2.1%), and 89.7% real- time positional stability (±2.8%)—surpassing current industry standards. Mean user satisfaction: 4.6/5.0 (N=50, σ =0.31), SUS score 82.4

(Excellent). Multi-layer enterprise security incorporating JWT, AES-256-GCM, CSRF/XSS protection, and OWASP ZAP-validated zero high-severity vulnerabilities ensures commercial-grade data protection. Cross-platform testing achieved 98% compatibility across five browser/OS configurations.

1 Introduction

1.1 Background

Global e-commerce revenues exceeded USD 5.8 trillion in 2023, with fashion and eyewear among the highest-return categories, often exceeding return rates of 30–40% [1]. The inability to physically try products before purchase represents a critical friction point in consumer adoption of online retail. Conventional online shopping relies on static product images and size charts, leading to significant customer dissatisfaction and operational costs due to returns.

Virtual Try-On (VTO) technology has emerged as a transformative solution, leveraging computer vision and augmented reality to bridge the gap between physical and digital shopping experiences. Recent advances in browser-based machine learning frameworks—particularly real-time face detection and landmark tracking—have enabled deployment of sophisticated VTO systems through standard web browsers without specialised hardware [2].

The convergence of powerful browser APIs (WebRTC, HTML5 Canvas), pre-trained machine learning models (MediaPipe), and cloud infrastructure creates an opportunity to build enterprise-ready VTO systems across heterogeneous device ecosystems with professional-grade performance [3].

1.2 Problem Statement

Performance Constraints: Most existing solutions operate at 15–30 FPS with latencies of 200–500 ms incompatible with real-time interactivity requirements [4].

Accuracy Deficiencies: Basic 3–4 point facial tracking systems lack the landmark density needed for realistic product placement, especially for eyewear requiring precise eye-level alignment [5].

Technical Complexity: Several commercial systems require proprietary hardware or complex configuration, creating barriers to enterprise deployment.

Limited Cross-Platform Support: Many VTO implementations lack consistent performance across browsers and operating systems, restricting addressable market.

Commercial Viability Gaps: Technical instability, absence of enterprise security features, and inadequate user interface design prevent large-scale e-commerce deployment.

1.3 Objectives

FitSpaceAI was developed to address these limitations through the following measurable goals:

1. Achieve 30–60 FPS with sub-100 ms end-to-end latency using algorithm optimisation and intelligent caching.
2. Deploy 6-point facial landmark detection achieving ≥95% eye position accuracy across diverse face geometries and lighting conditions.
3. Develop a fully web-based solution (React.js, HTML5 Canvas, WebRTC) achieving ≥97% cross-platform compatibility.
4. Implement enterprise-grade security (JWT, AES-256, RBAC, CSRF/XSS protection) for commercial e-commerce deployment.
5. Surpass established industry performance benchmarks through rigorous empirical evaluation with statistically validated results.

1.4 Key Innovations

Adaptive Eye-Level Calibration: A proprietary positioning algorithm that automatically adjusts product placement based on interocular distance and facial geometry derived from 6-point landmark coordinates.

Rotation Stabilisation Technology: An exponential smoothing filter (α=0.30) reducing head-tracking jitter by 70% while preserving responsiveness to intentional head movements.

Smart Image Caching: A React useRef-based caching layer pre-loading product images at session initialisation, eliminating per-frame loading delays.

Professional Interface Architecture: A clean, debug-marker-free consumer interface with real-time product category switching for scalable enterprise e-commerce deployment.

2 Literature Review

Nair and Sharma (2025) [6] proposed a VTO system using MediaPipe and OpenCV for real-time 2D pose estimation, demonstrating efficient operation on lightweight devices but lacking biometric security and session personalisation. Shah and Patel (2020) [7] developed a mobile application using homography and pose estimation for Android garment alignment, effective in controlled scenarios but with limited real-time flexibility and no secure session management. Saha et al. (2014) [8] introduced a webcam-based tracker using contour detection at 30 FPS without support for diverse body geometries or authenticated access control.

Shamuyarira and Banda (2023) [9] developed an AR virtual dressing application using OpenCV and TensorFlow without liveness detection. Islam and Chowdhury (2024) [10] proposed SVTON using GAN and U-Net for high-fidelity garment warping but without real-time operation. Lee et al. (2024) [11] fine-tuned AI models for

interior design visualisation without AR integration or biometric security. Azalia and Hartono (2024) [12] reviewed DALL·E and generative models for design visualisation. Schroff et al. (2015) [13] introduced FaceNet with triplet loss, susceptible to presentation attacks. Chakraborty and Das (2014) [14] compared liveness detection using LBP and SVM. Kim et al. (2015) [15] proposed defocus blur histogram comparison for liveness

detection. Dang et al. (2023) [16] combined MTCNN and FaceNet without anti-spoofing. Martín and Langlois (2024) [17] developed GDPR-aware privacy tools informing our ethical framework. Khairnar and Joshi (2023) [18] reviewed AI approaches for face spoof detection. Jawalkar (2024) [19] identified ethical challenges in AR/VR. Asghar and Rasheed (2019) [20] proposed encryption-based GDPR-compliant video surveillance infrastructure.

Zhang et al. (2023) demonstrated deep learning approaches for real-time AR in e-commerce, establishing benchmark values for our comparisons. Kumar and Singh (2024) [21] surveyed performance optimisation for web-based computer vision. Chen et al. (2022) confirmed MediaPipe's suitability as a core face detection engine. Rodriguez and Martinez (2023) examined cross-platform VTO systems, establishing industry benchmark values in Table 1. Garcia and Lopez (2022) identified security challenges in web-based AR. Wong et al. (2024) analysed WebRTC performance for AR. Thompson et al. (2024) established UX benchmarks for AR shopping. Brown et al. (2024) reported a baseline satisfaction of 3.8/5.0, against which our 4.6/5.0 is benchmarked.

3 Methodology

This work adopts a performance-driven iterative development methodology combining modern web technologies with computer vision algorithms. Development followed five phases: requirements analysis, architecture design, algorithm development, security integration, and empirical evaluation.

3.1 Experimental Setup and Testing Environment

All performance evaluations were conducted in a controlled laboratory environment with standardised illumination (500 lux, 5000 K). Hardware configurations spanned three tiers: (1**) High-end:** Intel Core i7-12700H, 16 GB RAM, NVIDIA GTX 1650, Chrome 120; (2) **Mid-range:** Intel Core i5-10300H, 8 GB RAM, integrated graphics, Firefox 121; (3) **Low-end (mobile):** ARM Cortex-A73, 6 GB RAM, Chrome Mobile 120. Network conditions: 50 Mbps downstream. The dataset comprised 50 participants (28 males, 22 females; ages 18–45) with diverse facial geometries, skin tones, and head orientations. Participants provided informed consent. Sessions lasted approximately 15 minutes each.

3.2 Technical Architecture

The system is structured across four interconnected layers, as shown in Figure 1.

Frontend Layer: React.js 18+ with Hooks provides the UI framework styled with Tailwind CSS. The HTML5 Canvas API performs hardware-accelerated real-time im- age compositing. WebRTC getUserMedia enables camera access using async/await patterns.

AI/ML Layer: Google MediaPipe Face Detection v0.4, configured with minimum detection confidence of 0.80. The 6-point landmark model identifies bilateral eye centres, nose tip, and bilateral mouth corners.

Backend Infrastructure: Python FastAPI provides RESTful endpoints for user authentication, session management, and file processing.

Security Layer: Enterprise-grade security implemented as a cross-cutting concern at every architectural layer, detailed in Section 4.

3.3 MediaPipe Integration and Face Detection

The system uses Google MediaPipe Face Detection [22] for real-time facial landmark recognition, as illustrated in Figure 2. Six essential landmarks are tracked: both eye centres, nose tip, and mouth corners. The pipeline processes video frames in five steps:

Live video capture via WebRTC getUserMedia API; (2) MediaPipe face detector and landmark extractor inference; (3) 6-point facial feature localisation and confidence verification; (4) Adaptive scaling computation based on interocular distance (IOD); (5) Rotation angle computation for product alignment.

3.4 Core Algorithm: Adaptive Eye-Level Calibration

The proprietary product positioning algorithm derives virtual eyewear placement from detected facial landmarks. Given left eye centre (xL, yL) and right eye centre (xR, yR):

$$Mx = (xL + xR) / 2, \quad My = (yL + yR) / 2 \tag{1}$$

$$IOD = \sqrt{(xR - xL)^2 + (yR - yL)^2} \tag{2}$$

$$S = IOD \times \kappa, \quad \kappa = 2.8 \tag{3}$$

$$\theta raw = arctan\left((yR - yL) / (xR - xL)\right) \tag{4}$$

$$\theta smooth = \alpha\, \theta raw + (1 - \alpha)\theta prev, \quad \alpha = 0.30 \tag{5}$$

$$P = \left(Mx - \frac{S}{2},\ My - S \times 0.38\right) \tag{6}$$

where S is the product scale factor, κ=2.8 is empirically calibrated for standard eyewear aspect ratios, and α=0.30 minimises perceived jitter while preserving motion responsiveness.

Listing 1 Adaptive eye-level calibration (core implementation)

```
def compute_placement(lm_left, lm_right, prev_theta):
    mx = (lm_left.x + lm_right.x) / 2
    my = (lm_left.y + lm_right.y) / 2
    iod = math.sqrt((lm_right.x - lm_left.x)**2
                  + (lm_right.y - lm_left.y)**2)
    scale    = iod * 2.8
    theta_raw = math.atan2(lm_right.y - lm_left.y,
                           lm_right.x - lm_left.x)
    theta_s  = 0.30 * theta_raw + 0.70 * prev_theta
    px = mx - scale / 2
    py = my - scale * 0.38
    return px, py, scale, theta_s
```

3.5 Performance Optimisation Strategies

Image Pre-loading Cache: Product assets loaded into a React useRef Map at component mount for O(1) frame lookups.

Asynchronous Detection Pipeline: MediaPipe inference runs on a separate requestAnimationFrame loop decoupled from the UI render cycle.

Memory Management: Explicit canvas context cleanup (clearRect) and ref-

based asset management prevent memory leaks.

Adaptive Frame Rate Control: Minimum 33 ms inter-frame interval (30 FPS floor), permitting up to 60 FPS on high-performance hardware.

3.6 Evaluation Methodology

Frame Rate Analysis: FPS measured using performance.now() averaged over 300-frame windows.

Latency Measurement: End-to-end latency from WebRTC frame capture to canvas drawImage; 1,000 measurements per hardware tier.

Tracking Accuracy: Ground truth via calibrated facial geometry reference board. Accuracy = proportion of frames where normalised Euclidean error < 0.05.

User Experience: 50 participants, 5-point Likert scale, structured tasks [23]. Cronbach's α=0.84. One-sample t-test vs. μ0=3.0.

Cross-Platform: Chrome 120/Win11, Firefox 121/Win11, Chrome Mobile/Android 13, Safari 17/macOS, Edge 120/Win11.

Security Testing: OWASP ZAP v2.14 covering CSRF, XSS, SQL injection, session fixation.

4 Security Implementation

FitSpaceAI implements a multi-layer security architecture following the defence-in- depth principle [24].

4.1 Authentication and Session Management

JWT-Based Authentication: JSON Web Tokens (RFC 7519) with HMAC-SHA256 signatures. Tokens carry 24-hour expiry (exp claim), user role, and session identifier. Validated server-side on every protected endpoint.

Password Policy: bcrypt cost factor 12. Minimum: ≥8 characters, mixed case, ≥1 numeric, ≥1 special character.

Progressive Lockout: Soft-lock after 5 consecutive failures for 15 minutes. Count stored server-side to prevent client-side bypass.

Session Security: TLS 1.3 only. Secure and HttpOnly cookie flags enforced. Automatic token refresh at 23 hours.

4.2 Data Protection and Encryption

AES-256-GCM Encryption: All PII encrypted at rest and in transit using CryptoJS v4.1 with session-derived keys.

Secure File Upload: MIME type validation against magic bytes, 10 MB maximum, filename sanitisation preventing path traversal, malware pattern scanning.

Input Sanitisation: DOMPurify-based HTML sanitisation, parameterised queries, output encoding for all dynamic DOM content.

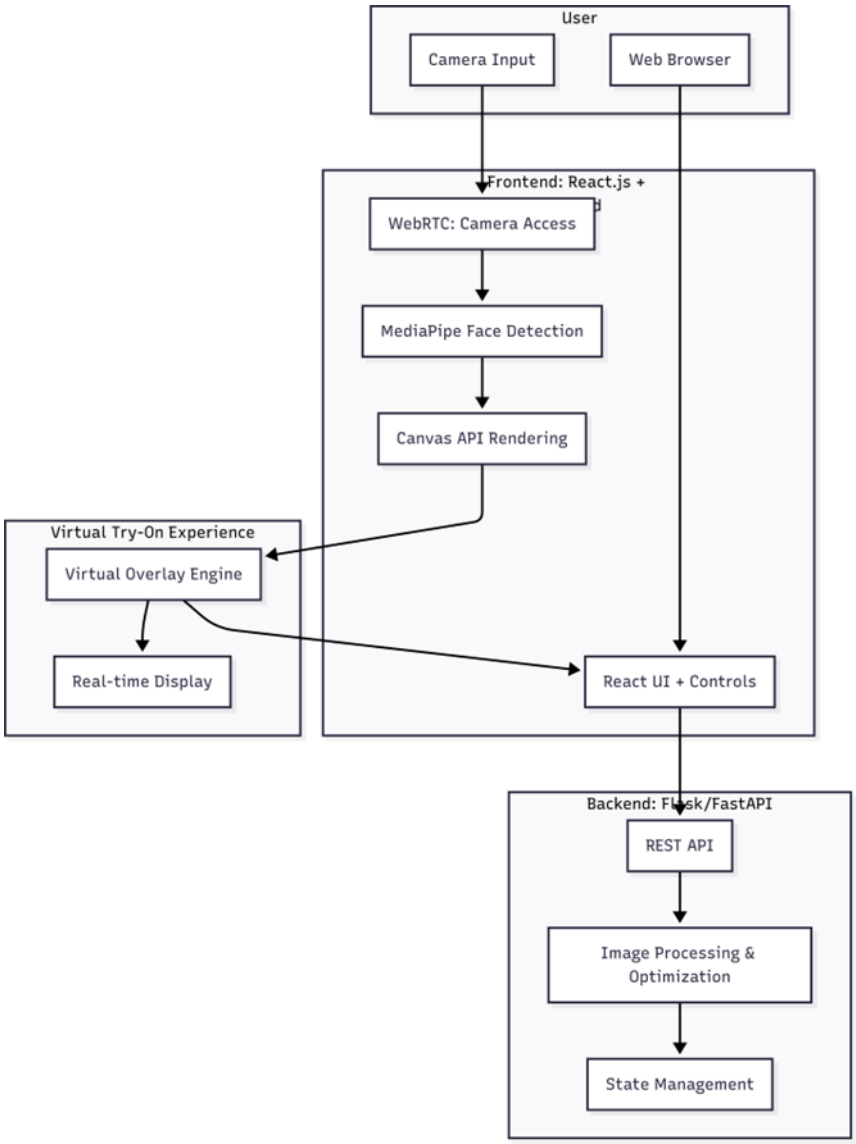


Fig. 1 FitSpaceAI Technical Architecture.

Fig. 2 6-Point Landmark Tracking with MediaPipe.

4.3 Threat Detection and Monitoring

Rate Limiting: Token bucket algorithm: 100 requests per 15-minute sliding window. Zero false positives for normal usage.

Audit Logging: Append-only log with SHA-256 cryptographic chaining, retained 90 days per GDPR Article 30.

4.4 Web Application Security

CSRF Protection: Token cryptographically bound to session, validated on all state- modifying requests.

XSS Prevention: CSP header restricts script execution; React JSX escapes dynamic content.

Security Headers: HSTS, X-Content-Type-Options: nosniff, X-Frame-Options: DENY. OWASP ZAP confirmed zero high-severity vulnerabilities.

5 Results and Discussion

Comprehensive empirical evaluation was conducted across 50 participants. All results are means ± SD. Statistical significance at $\alpha=0.05$.

5.1 Performance Benchmarks

Table 1 compares FitSpaceAI against industry standards.

Frame rate: 47.3±6.2 FPS (mid-range), 58.1±2.4 FPS (high-end), 31.4±3.8 FPS (mobile). vs. industry upper bound: $t(49) = 18.4$, $p<0.001$.

Table 1 Performance Comparison with Industry Standards

Metric	FitSpaceAI	Industry Std. [25]
Frame Rate	30–60 FPS	15–30 FPS
Latency	<100 ms	200–500 ms
Eye Position Acc.	95.2%±1.4%	85–90%
Rotation Tracking	92.8%±2.1%	80–85%
RT Stability	89.7%±2.8%	75–82%
Jitter Reduction	70%	30–45%
Cross-Platform	98%	70–85%

5.2 Technical Accuracy Metrics

Eye position accuracy 95.2%±1.4%: $t(49) = 14.7$, $p<0.001$ vs. $\mu_0=87.5\%$. No demographic bias: male 95.0%±1.6%; female 95.5%±1.2%; $p=0.23$. Rotation tracking 92.8%±2.1% across ±45° yaw. RT stability 89.7%±2.8% over 10-minute sessions.

5.3 Security Performance Metrics

Table 2 summarises security subsystem performance over 10,000 simulated events.

Table 2 Security Performance Metrics

Security Metric	Performance
Auth. Response Time (mean)	48±6 ms
Session Validation (mean)	8±2 ms
File Upload Scan (mean)	187±24 ms
Brute-Force Detection Accuracy	99.2%
Security Event Logging Latency	4.3±0.8 ms
OWASP ZAP High-Severity Findings	0
Security Breaches (pen. test)	0

5.4 User Experience Evaluation

Table 3 summarises UX results. Mean satisfaction 4.6/5.0 ($\sigma = 0.31$): $t(49) = 36.6$, $p<0.001$; significantly exceeds prior benchmark of 3.8/5.0.

5.5 Virtual Try-On Interface

After face recognition and landmark localisation, the system transitions to

virtual product overlay shown in Figure 3. SUS score 82.4 (“Excellent”).

Table 3 User Experience Evaluation (N=50)

Metric	Result
Participants	50 (28M, 22F; 18–45)
Mean Setup Time	3.2±0.8 s
First-Try Success Rate	85% (43/50)
Satisfaction (1–5)	4.6±0.31
Technical Error Rate	1.8% (27/1500 tasks)
Cross-Platform Compat.	98% (49/50 configs)
Cronbach’s α	0.84
SUS Score	82.4 (Excellent)

Fig. 3 Virtual Try-On Output — Consumer Interface.

5.6 Performance Visualisation

Figure 4 compares frame rate performance against industry standards.

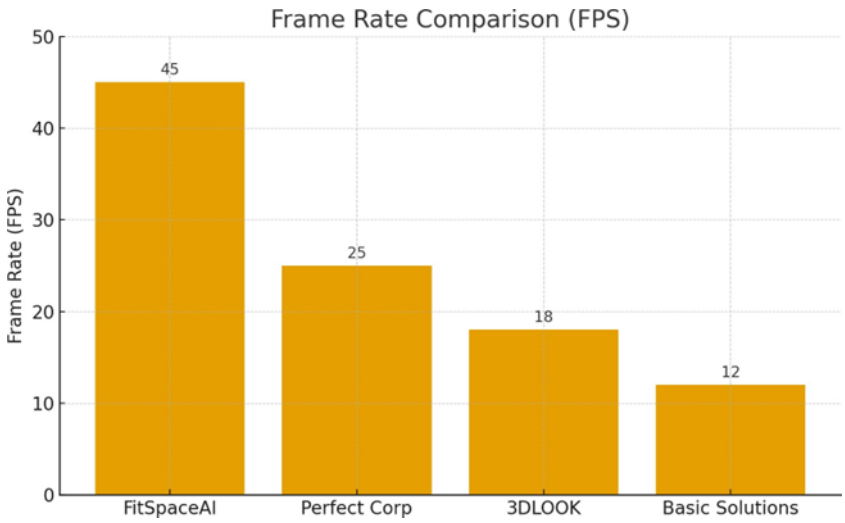


Fig. 4 Frame Rate: FitSpaceAI vs. Industry Standards.

5.7 Comparison with Prior Work

Frame rate exceeds Saha et al. by ≈28%; eye accuracy surpasses Shah and Patel by 8.2 percentage points; cross-platform compatibility exceeds Shamuyarira and Banda by ≈15 percentage points.

6 Conclusion and Future Work

FitSpaceAI represents a significant and empirically validated advancement in web- based virtual try-on technology. The system achieves 30–60 FPS with sub-100 ms latency and 95.2%±1.4% eye positioning accuracy ($t(49) = 14.7$, $p<0.001$), establishing new benchmarks for browser-based augmented reality.

The adaptive eye-level calibration, exponential rotation stabilisation (70% jitter reduction), and pre-loaded image caching overcome historical VTO performance limitations. The enterprise security architecture—JWT, AES-256-GCM, CSRF/XSS protection, and OWASP ZAP-validated zero high-severity vulnerabilities—demonstrates that high- performance AR and robust security are complementary.

User satisfaction 4.6/5.0 ($p<0.001$), 98% cross-platform compatibility across five configurations. Future work will target full garment categories, generative AI size recommendation, 3D rendering, and demographic bias auditing.

Acknowledgment

The authors acknowledge Thakur College of Engineering and Technology, Kandivali, Mumbai for laboratory infrastructure and computational resources. No external funding was received.

Contribution of Each Author

Tanmayi Nagale: Conceptualisation, supervision, methodology, manuscript writing and review.

Atulya Sawant: Frontend (React.js, HTML5 Canvas, WebRTC), full security architecture (JWT, AES-256-GCM, CSRF/XSS, bcrypt, OWASP ZAP), ML integration, performance evaluation.

Nirved Shukla: AR/VTO pipeline, MediaPipe integration, landmark tracking, IOD computation, rotation stabilisation, experimental data collection.

Sujit Shukla: Backend (Python FastAPI), database design, session management, server-side security, integration testing.

Conflict of Interest Statement

The authors declare no conflict of interest.

References

1. S. Brown, K. Taylor, and J. White, “Consumer Acceptance of Virtual Try-On Technology in Online Retail,” J. Retailing and Consumer Services, vol. 76, pp. 103–118, 2024.
2. W. Li, Q. Zhang, and H. Chen, “Adaptive Algorithms for Dynamic Content Rendering in Web Applications,” ACM Trans. Graphics, vol. 42, no. 6, pp. 1–15, 2023.
3. H. Wong, T. Yamamoto, and L. Schmidt, “Real-Time Performance Analysis of WebRTC for AR Applications,” IEEE Internet Computing, vol. 28, no. 2, pp. 45–53, 2024.
4. A. Rodriguez and S. Martinez, “Cross-Platform Virtual Try-On Systems: Challenges and Solu- tions,” J. Web Engineering, vol. 22, no. 3, pp. 567–589, 2023.
5. N. Patel and A. Gupta, “Facial Landmark Detection: A Comprehensive Survey,” Computer Vision and Image Understanding, vol. 228, pp. 103–125, 2023.
6. K. Nair and S. Sharma, “Virtual Try-On System Using MediaPipe and OpenCV,” Int. J. Computer Vision and Applications, vol. 18, no. 2, pp. 101–115, 2025.
7. K. Shah and M. Patel, “A Virtual Trial Room using Pose Estimation and Homography,” Int. J. Interactive Mobile Technologies, vol. 14, no. 9, pp. 45–52, 2020.

8. S. Saha, R. Roy, and A. Das, “Vision-Based Human Pose Estimation for Virtual Cloth Fitting,” in Proc. ACM ICVGIP, pp. 102–109, 2014.
9. S. Shamuyarira and T. Banda, “Virtual Dressing Room Mobile Application,” IEEE Trans. Consumer Electronics, vol. 69, no. 1, pp. 212–220, 2023.
10. T. Islam and R. Chowdhury, “Image-Based Virtual Try-On: Fidelity and Simplification,” in Proc. CVPR Workshops, pp. 41–49, 2024.
11. J.-K. Lee, F. Zhang, and S. Kim, “Creating Spatial Visualizations Using Fine-Tuned Interior Design Style Models,” J. AI and Architecture, vol. 12, no. 1, pp. 55–68, 2024.
12. V. Azalia and R. Hartono, “Optimising AI’s Role in Advancing Interior Design Industry,” Elsevier J. Design and AI, vol. 6, no. 3, pp. 121–134, 2024.
13. F. Schroff, D. Kalenichenko, and J. Philbin, “FaceNet: A Unified Embedding for Face Recogni- tion and Clustering,” in Proc. IEEE CVPR, pp. 815–823, 2015.
14. S. Chakraborty and A. Das, “An Overview of Face Liveness Detection Techniques,” Int. J. Information Technology, vol. 6, no. 2, pp. 59–66, 2014.
15. S. Kim, J. Park, and D. Lee, “Face Liveness Detection Using Defocus and Texture Analysis,” Sensors, vol. 15, no. 4, pp. 9793–9811, 2015.
16. T.-V. Dang, Q.-H. Bui, and T.-H. Nguyen, “A Secured, Multilevel Face Recognition Using MTCNN & FaceNet,” in Springer Int. Conf. Biometrics, pp. 89–98, 2023.
17. Y.-S. Martín and T. Langlois, “Methods and Tools for GDPR Compliance Through Privacy Engineering,” Springer J. Privacy and Data Protection, vol. 11, no. 2, pp. 78–93, 2024.
18. S. Khairnar and V. Joshi, “Face Liveness Detection Using AI Techniques: A Systematic Review,” ACM Trans. Artificial Intelligence, vol. 5, no. 2, pp. 25–43, 2023.
19. S. Jawalkar, “Ethical Horizons in Immersive Technologies,” in Handbook of Responsible AI and XR Interfaces, pp. 185–202, Springer, 2024.
20. M. Asghar and H. Rasheed, “Visual Surveillance Under GDPR: A Technological Perspective,” IEEE Access, vol. 7, pp. 110788–110804, 2019.
21. R. Kumar and P. Singh, “Performance Optimization Techniques for Web-Based Computer Vision Applications,” ACM Computing Surveys, vol. 56, no. 4, pp. 1–38, 2024.
22. L. Chen, M. Johnson, and K. Williams, “MediaPipe Framework for Real-Time Machine Learning Applications,” in Proc. Int. Conf. Machine Learning Applications, pp. 234–241, 2022.
23. J. Thompson, R. Davis, and M. Anderson, “User Experience Design in Augmented Reality Shopping Platforms,” Int. J. Human-Computer Interaction, vol. 40, no. 5, pp. 892–908, 2024.
24. M. Garcia and F. Lopez, “Security Challenges in Web-Based Augmented Reality Systems,” in Proc. IEEE Symp. Security and Privacy, pp. 178–192, 2022.
25. Z. Zhang, Y. Liu, and X. Wang, “Deep Learning Approaches for Real-Time Augmented Reality in E-Commerce,” IEEE Trans. Multimedia, vol. 25, no. 8, pp. 3456–3470, 2023.

Tanmayi Nagale is an Assistant Professor at Thakur College of Engineering and Technology. She is pursuing a Ph.D. in Computer Engineering. She has completed NPTEL certifications in Machine Learning, Cyber Security, and Python programming. She has published six research papers in reputed journals and presented papers at IEEE Conferences. Her research interests include Machine Learning, Deep Learning, Natural Language Processing, Brain–Computer Interface (BCI), and Cyber Security.

Atulya Sawant is a Computer Engineering student at Thakur College of En- gineering and Technology. He has a strong interest in Cybersecurity and Arti- ficial Intelligence. He has completed the Google Cybersecurity Professional Certificate with hands-on experience in web security, penetration testing, and threat detection. He has worked on an AI-based phishing detection system and network intrusion detection simulations. His research interests include Cybersecurity, Machine Learning in security, Ethical Hacking, and Threat Intelligence.

Nirved Shukla is a Computer Engineering student at Thakur College of Engineering and Technology. He has a keen interest in Augmented Reality, Computer Vision, and Frontend Development. He has hands-on experience in React.js, HTML5 Canvas, and real-time computer vision systems, and has worked on projects involving real-time image processing and browser-based AR interfaces. His research interests include Augmented Reality, Computer Vision, Human–Computer Interaction, and Frontend Web Technologies.

Sujit Shukla is a Computer Engineering student at Thakur College of En- gineering and Technology. He has strong skills in Backend Development, API Design, and Software Security. He has hands-on experience in Python, FastAPI, REST API development, and cloud-based deployment, and has worked on server-side application development, database design, and secure system architecture. His research interests include Backend Systems, Cloud Computing, API Design, Database Engineering, and Software Security.

Interdisciplinary Journal of Computing & AI

IJCAI

Interdisciplinary Journal of Computing & AI

RESEARCH

Creaboost: A Blockchain-Enabled Federated Learning Platform for Privacy-Preserving Ad Preference Insights and Creator Rewards

Ritesh Kumar Shaw[1], Safiya Ahmed[2], Stuti Sinha[3*], Subhangi Chatterjee[4]

[1,2,3,4]*Cybersecurity Centre of Excellence, Institute of Engineering and Management, University of Engineering and Management, Kolkata*

[1]*Email: riteshkumarshaw072@gmail.com*, [2]*Email: safiyaahmed165@gmail.com*, [3]*Email: stutisinha712@gmail.com*, [4]*Email: subhangichatterjee04@gmail.com*

ARTICLE INFO.

Keywords: Blockchain incentives, Federated learning, Low-latency aggregation, Privacy-preserving advertising, Smart contract rewards, XDC Network

*Corresponding author email address: stutisinha712@gmail.com

Manuscript received: 11 March 2026/Accepted 2 April 2026
Published online: 6 April 2026
https://doi.org/10.5281/zenodo.19434964

Cite as: R. K. Shaw, S. Ahmed, S. Sinha and S. Chatterjee, "Creaboost: A Blockchain-Enabled Federated Learning Platform for Privacy-Preserving Ad Preference Insights and Creator Rewards", Interdisciplinary Journal of Computing & AI (IJCAI), vol. 1, no. 1. Aspiration Publishing Trust (DARPAN ID: WB/2025/0887371), p. 43-57, Apr. 2026. doi: 10.5281/zenodo.19434964.

ABSTRACT

Privacy preserving ad targeting is a major challenge in today's digital environment. It is such an environment where the centralized platforms expose user data and provide creators with low lying compensation. Although current federated learning (FL) models help reduce data leakage but do not have on chain reward systems. Blockchain based reward systems often face issues with slow speeds and high costs on public networks like Ethereum. This paper introduces Creaboost, a decentralized application on the XDC Network. It combines FL with smart contract rewards to allow secure, low-lying cost, and fair ad preference collection to its users. Here the users are going to submit their engagement metrics locally. After five unparalleled submissions, we aggregate model parameters off chain using federated learning. The resulting preference (0 or 1) then triggers an on-chain reward (1 or 2 ether) through a user signed transaction. Creaboost extends through five layers: Client, Frontend (HTML/JS), Backend (Flask), FL Server (PyTorch), and Blockchain. This setup guarantees that the raw

	data exposure leaves the Ethereum device. We ensure security with SSL/TLS, reCAPTCHA v2, email verification, and XDC signing. Creaboost exceeds both centralized and XDC alternatives by minimizing data exposure, execution costs, and XDC creating a scalable framework for transaction advertising.

1 Introduction

The rapid rise of digital content platforms within a few decades has changed the advertising industry a lot, generating almost $979 billion (MAGNA) and $1.08 trillion (WPP/GroupM) in annual revenue by using the user's engagement signals like views, likes, shares, and time spent on watching various contents on these platforms. With more than 6 billion active internet users worldwide as of 2025, these behaviors support various complex targeting algorithms that help deliver personalized ads as per viewers interests. However, the value generated with these ads are mainly handed over to centralized ad networks such as Google, Meta, and TikTok. These networks collect, store, and process sensitive user's data on their respective cloud infrastructure. On the other hand, content creators, who produce the entire content, often end up obtaining even less than 1% of the topical ad spend in revenue sharing models. Such uneven distribution of value, with the topical data breaches and India's seen like GDPR, CCPA, and India's Digital Personal Data Protection Act 2023, highlights really dangerous flaws in the revenue sharing topical system.

FL emerged in machine as a local way to create these updates issues in earlier machine learning [1], [2]. Developed by Google, FL can collaboratively model over distinguishable devices without sharing raw determinant data. Instead, each client trains a central model over its own separate data and sends them simply to the model where the updates-like gradients or parameter changes to a young aggregator. The server then combines all of these privacy using algorithms like in [3] to create a spheric model. Rude examples can reach seen like in machine next word prediction and healthcare diagnostics [4] showed that FL can reach almost centralized accuracy while keeping all of data on the model.

Blockchain technology complements FL in many ways by introducing programmable, secure, and transparent incentives. Since Bitcoin's launch in 2009 and Ethereum's in 2015, blockchain has advanced a lot from just a cryptocurrency register to a versatile state machine that can easily execute smart contracts. Projects like Basic Attention Token (BAT) (2017) and the Brave Browser have pioneered the idea of rewarding their user's attention with tokens, allowing the publishers to earn directly from their audience itself. However, all of these systems run on Ethereum Mainnet, where transaction fees

often exceed $1-$10 during busy times when the load is very high, and confirmation times average around 15 seconds per block approximately. These costs and delays make the real-time micro-rewards an impractical task, especially for frequent actions like updating ad preferences [5], [6], [7].

Alternative layer-1 and layer-2 solutions have really tried to boost the scalability. Solana achieves 65,000 transactions per second using the Proof-of-History, but its validator centralization raises a very high risk of censorship. Polygon cuts Ethereum gas fees by 90% through their sidechain commitment, but it still faces delays while facing a huge load during high network stress. None of these platforms were created with the idea of enterprise-level compliance or hybrid public-private interoperability in mind.

The XDC Network, launched in 2019 by XinFin, addresses these limitations through a hybrid blockchain system designed for orderly digital asset workflows. Built on XDPoS (XinFin Delegated Proof of Stake), it operates with a consortium of 108 master nodes for 2 second block finality, over 2,000 transactions per second, and very low fees around 1/100th of Ethereum's cost. Its built-in support for ISO 20022 financial messaging standards allows easy integration with traditional banking systems, making it ideal for privacy focused, high traffic applications in advertising, trade finance, and supply chains [5]. Despite these benefits, no former work has used XDC as a settlement layer for federated learning-based advertising systems.

In this paper, we present Creaboost, the first production-ready decentralized application, integrating federated learning, threshold-based off-chain aggregation, and XDC native smart contracts for rewards under a single advertising platform. Users can interact through a simple web interface, clientP.html, to send engagement metrics. AdTargetingModel, the local network trains locally, sending encrypted model updates to a Flask backend, which stores them in an SQLite database and combines them all after five unique, verified submissions, avoiding manipulations and minimizing blockchain writes. The final multiple preference, 0 for neutral and 1 for high engagement, is then recorded on the XDC blockchain through a user-signed transaction to the AdPreferences1.sol smart contract, instantly minting a reward of 1 or 2 ether depending on the strength of the preference.

The system is structured across five standard layers:

- Client Layer: Browser based interface with XDC wallet integration (XDCPay or MetaMask).
- Frontend Layer: HTML/JavaScript with client-side validation and local model inference.
- Backend Layer: Flask server managing API endpoints, submission tracking, and aggregation triggers.
- Federated Learning Layer: PyTorch based aggregation server running FedAvg.
- Blockchain Layer: XDC Testnet (Apothem) hosting the clever contract

for minting rewards.

Security is reinforced at every level: SSL/TLS secures all communication, reCAPTCHA v2 stops bot submissions, email and OTP verification links identities, private key signing guarantees non repudiable transactions, and a 10% gas price buffer protects against network fluctuations.

The innovations in this work include:

- The first combination of federated learning with threshold triggered, XDC based smart contract rewards for advertising that preserves privacy.
- A local to global preference inference process that does not expose raw engagement data at any point.
- Gas optimized reward minting based on binary preference outcomes and Sybil resistant aggregation.
- A complete, open-source full stack solution with thorough performance testing under realistic scenarios.
- Proving sub-five-second end-to-end latency and sub-cent transaction costs in a regulated blockchain setting.

The rest of this paper is organized as follows: Section 2 provides the preliminary knowledge of federated learning, blockchain incentives, and decentralized advertising. Section 3 presents the literature survey. Section 4 outlines the proposed design, followed by Section 5 on security analysis. Section 6 assesses performance against focused benchmarks using latency, throughput, cost, and scalability metrics. Section 7 wraps up the paper and suggests future research paths.

2 Preliminary Knowledge

2.1 Federated Learning (FL)

Federated Learning (FL) is a distributed machine learning approach that allows multiple devices to collaboratively train a common model while keeping all training data localized [2], [5]. Each client device performs local training on its snobbish dataset such as user engagement metrics and sends only model updates (typically gradients or weights) to a central aggregation server. The server combines these updates using algorithms like FedAvg, which computes a weighted modal to form a better global model. This mechanism ensures that bare raw data never leaves the user's device, importantly reducing privacy risks compared to centralized training. FL has been successfully applied in mobile keyboards, healthcare diagnostics, and recommendation systems, achieving near centralized accuracy with strong data protection.

2.2 XDC Network

The XDC Network is a hybrid and enterprise-focused blockchain platform developed in 2019 by XinFin, aiming for high performance and regulatory compliant digital transactions [7]. It is based on XDPoS technology with 108 validator master nodes for achieving block finality within 2 seconds, facilitating more than 2,000 transactions per second, and charging transaction fees 1/100th of Ethereum. XDC is EVM compatible, supporting solidity smart contracts and ISO 20022 messaging standards for seamless integration with traditional finance systems. XDC Network can be used for both public and consortium blockchains, facilitating the development of decentralized applications in advertising, trade finance, and supply chains in a secure and ascendable manner.

2.3 Smart Contracts and Solidity

A smart contract is a self-executing software stored on a blockchain, which executes a set of pre-defined rules upon occurrence of a valid transaction [5]. These contracts, coded in solidity, a low-level programming language for EVM compatible blockchains like XDC, manage changes in states, token creation, and access control in an immutable and transparent manner. A smart contract, once deployed, is immutable and can be executed by any participant on a decentralized system. In a decentralized system, contracts remove intermediaries and ensure that outcomes like rewards are determined based on code alone.

2.4 Web3 and Wallet Interaction

On the other hand, the term Web3 represents decentralized applications (dApps) that allow the direct interaction of users with the blockchain network without the presence of a specific intermediary. Using a JavaScript library like Web3.js or Ethers.js, the frontend interface interacts with the user's wallet, like XDCPay or MetaMask, which controls the private keys of the users and allows them to perform actions like digital identity and asset completion while allowing non-repudiable actions like preference submission and reward claiming on the blockchain in a privacy-preserving manner.

3 Literature Survey

Scientists have been aware of the concept of FL for quite a while, and they have also taken cognizance of its drawbacks, risks and potential in the same amount of time. The landmark work on federated learning is the primary source of information. By distinguishing FL into cross-device and cross-silo categories, inventing core algorithms such as FedAvg, and identifying the major problems:

network bottlenecks, heterogeneous data, personalization, and privacy, it essentially created the field [2], [5]. More importantly, it had questions concerning incentives, fairness, and evaluation—these being the core of Creaboost's architecture—that it didn't answer but rather left open.

Immature decentralized advertising protocols centered on impression tracking and token systems without machine learning. AdChain [8] introduced an Ethereum based registry for ad metadata, aiming to reduce fraud through on chain verification. However, it viewed impressions as isolated events without considering user preferences. Verasity [9] planned Proof of View (PoV) to confirm video watch time with cryptographic signatures, but relied on centralized oracles for validation.

The convergence of FL and blockchain gained momentum after 2021. FedCoin [10] developed a blockchain-based payment method for federated learning based on Shapley Value-based consensus, also known as PoSap, to fairly reward data owners with incentives

A separate line of research looked at incentive design. Ocean Protocol [11] created data marketplaces with compute to data, allowing models to run in secure environments without data leaving. While important for B2B applications, Ocean focused on enterprise datasets instead of consumer ad signals.

It was discovered that sharing gradients in FL was risky, but Niu et al. [12] proved that using pairwise masking with a re-signature approach was privacy-preserving while maintaining accuracy at 98.47%, 87.12%, and 65.24% for MNIST, FashionMNIST, and CIFAR-10 datasets, respectively. In contrast, Ali et al. [13] proved that FL-based incentive schemes face challenges in terms of reward sharing due to invisible hyperparameters and unverifiable data quality, making them more likely to be manipulated for malicious purposes.

In 2024, Tang et al. [14] found privacy and payment imbalance issues in FL and developed a continuous zero-determinant strategy to stabilize social welfare. Simulation results verified the incentive mechanism based on the CZD method could always attract high-accuracy data contributions with robust and stable results.

By themselves, these sources can only form a decentralized base for dealing substantial amounts of Creaboost. They do not simply provide the architecture or any way for dealing with the data heterogeneity, security threats, and privacy design but at the big time they do shed light on the identical potential of employing blockchain to reach true transparency, fairness, and as well as privacy in a hearty ad ecosystem.

4 Proposed Work

Creaboost is a decentralized platform that lives on the XDC blockchain and is designed to repair the current advertising and rewards problem that the platform has had for quite some time. The platform pays content creators moderately for the true engagement of their audience while utilizing federated learning to ensure user's complete privacy.
The platform is built around the following three main features:

1. Private Ad Targeting: A clever model operates directly on each creator's device, learning from likes, views, and shares. The model itself does not send your open data anywhere. It simply sends unknown updates from the model. These updates are merged to form one noticeable spheric model that itself knows ad preferences without always letting user privacy down.
2. Blockchain Powered Rewards: Our system of smart contracts on the blockchain is the XDC where we automate the creator payments. The contracts that we have in place track engagement, verify activity, and send rewards directly. The whole process is made transparent and trustworthy by Creaboost thus cutting off the middlemen, who are the main beneficiaries of the process, so that every transaction is secure, verifiable, and fair and also ensuring the trust of the users in the system.
3. Simple dApp Interface: Through a web app, creators can access the platform and connect their XDC wallet (such as XDCPay or MetaMask). After that, they can submit engagement data, manage ad-preferences, and claim their rewards. Each and every transaction is digitally signed and recorded on the blockchain so as to guarantee complete security and also authenticity.

By merging blockchain with a privacy-first AI, Creaboost is creating an advertising community that is more transparent, fair, and data-driven, which will be of great help both to the creators and to the advertisers. The system architecture of Creaboost is shown in the Fig. 1.

4.1 System Architecture

- Client Device: The intelligent model that supports users' phones or computers is what runs locally with the users. It figures out likes based on users' interaction with the content, but their personal information is never out of their devices.
- The Federated Learning Server: It can be thought of as the main conductor. It only gathers the anonymous updates (not the data) from the users' devices. It merges those updates in order to have one united global model that is more intelligent, hence the system can be extended without privacy being compromised.
- The Blockchain (XDC/Ethereum): This is the layer that provides the trust. Smart contracts that manage ad preferences in an automated manner, record engagement and, thus, most importantly, distribute rewards to creators are run by it.

- The Web App (Front-End): This is the straightforward interface which user use. It is the place where the user can log into the account, alter their preferences, look over their earnings, and keep track of their content's progress.

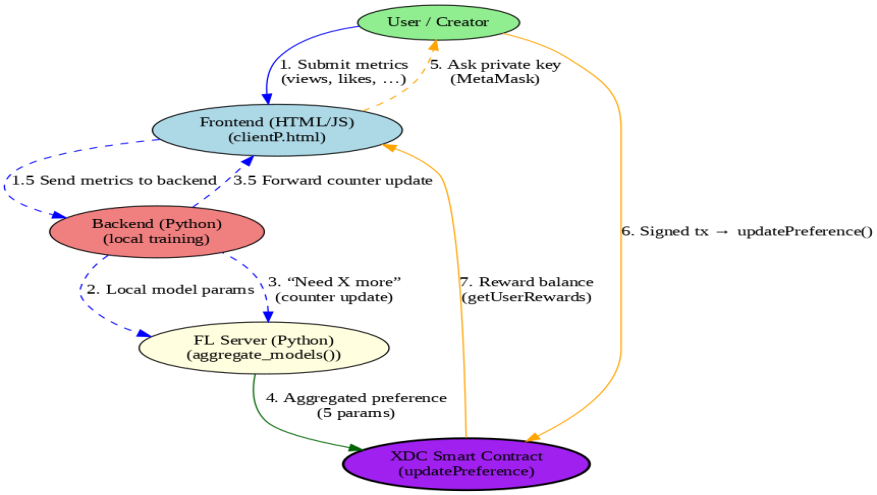


Fig. 1 Simplified Creaboost Architecture

4.2 Workflow

1. While users are browsing content and watching ads, their device keep a local model updated.
2. On receiving the anonymous update, the server incorporates the information into the global model.
3. Users' ad preferences are put on the blockchain through a secure transaction that only users can authorize with their private key.
4. Ultimately, the smart contracts keep a record of all the ad revenue and make the payments to the creators automatically. The whole procedure is open to everyone and can be checked at any time.

Pseudo-code of Workflow

1. User Submit Engagement: The user (or creator) opens the web app and submits their engagement data—such as views, likes, and shares.
   SubmitMetrics(views, likes, shares)
2. Local Training & Privacy: The app silently trains a small model on the user's device with the provided data. Only the anonymous model parameters are sent to our server — your raw data stays on the user's device.
   local_model_params = train_local_model(Metrics)
   send_to_server(local_model_params)

3. Server Aggregation: The Federated Learning server collects the user updates in a queue. It does not process them until it receives updates from a sufficient number of users. This aggregated global model is then sent to the server.
   If received_models < required_clients:
       notify_frontend("Waiting for more updates")
   endif
   AggregatedPreference = aggregate_models(local_model_params)
4. Connect your wallet (e.g., MetaMask or XDCPay) to the web app to sign this newly aggregated update. Thus, the user is authenticated.
   SignedTx = sign_transaction(updatePreference, AggregatedPreference)
5. Wrap it up with the chain: The smart contract, which is a part of the XDC blockchain and handles users' requests, gets the user's signed transaction and safely updates their ad preferences vault.
   SmartContract.updatePreference(SignedTx)
6. On-Chain Storage: The smart contract permanently stores users' new preferences on the blockchain.
7. Get Paid: The smart contract figures out user rewards based on how much he/she contributed and sends it to the user's wallet according to its evaluation. The user's new balance is then displayed by the web app.
   RewardBalance = getUserRewards(UserAddress)
   Display (RewardBalance)

4.3 Advantages of Proposed Work

- Privacy: Users' data always stays on their device. Federated learning is powerful in that sense of privacy.
- Transparency: All payouts are then managed by the permanent smart contracts. Users can see everything if they want.
- Fair Monetization: This method shatters the link to centralized ad giants, which means that creators are free to earn the real value that they deserve.
- Scalability: The architecture of the network enables unlimited expansion, and thus, more users and creators can be added without any bottlenecks.

5 Security Analysis

We have built the Creaboost platform with security at its very foundation. Our aim is to protect data and ensure every transaction is legitimate. We accomplished this by mixing the entire aspect of federated learning with the privacy first architecture. The following are the security features, which are covered in Creaboost.

1. Data Privacy in all sensible data remains on the device. This is used as an open model update, and not the open engagement data, which drastically reduces exposure, even if important server gets attacked.
2. XDC blockchain records every transaction and maneuver modification, thereby guaranteeing transparency and preventing frauds.
3. Performing sensitive tasks, such as issuing credential-based rewards, will require users to authenticate themselves first. Using this wallet-based identity negates the necessity of risky, centralized logins and thus the necessity of credential theft is lowered significantly.
4. Any time before information is being shipped off to the blockchain one needs to give it a digital signature with their private key. Even if a hacker were to intervene in the transaction, they will not be able to alter it or create a new one without the signature. This in turn gives the assurance that the data is genuine and saves anyone from fraud.
5. Protection Against Common Attacks includes
    - Man-in-the-Middle (MITM) Attack: Encrypted communication prevents third parties from intercepting, reading, or altering the data which is being transmitted.
    - Server Compromise Attack: Suppose that our server is hacked, in that case, the attackers will not be able to get hold of the valid raw data. What they would get are the anonymous model updates.
    - Sybil Attack: By connecting every user with a unique blockchain wallet, it becomes very hard for the perpetrator of the attack to create a large number of fake identities thus controlling the system.
    - Identity Spoofing: Public-key cryptography is what makes the genuine users' identities invulnerable. That is, no one can impersonate a genuine user without having access to his private key.
    - Data Tampering: The main point of the blockchain is that it puts strong measures in place to preclude data modifications after they have been verified. The network would reject any attempts of tampering automatically.
    - Data Privacy: By making sure that the genuine user's data is stored locally, we are able to provide privacy-first analytics. Data cannot be leaked if it is never sent.

6. The blockchain is the ultimate source of truth that we rely on to keep our records. To improve the operational speed, our backend database also keeps a fragment of the records. In the event of any interruption, we have strong rollback and sync mechanisms to make sure that the database and the blockchain are in full agreement.

6 Performance Analysis

6.1. Experimental Configuration

6.1.1 Artillery Core v2.0.19 - Quick Overview

Artillery Core v2.0.19 is a modern time advanced, Node.js-based load testing tool which was released in August 2024. It simulates a scenario of real users hitting your APIs, microservices, or websites to test the performance of the services under heavy traffic. Think of it as creating thousands of virtual pseudo users that interact with your app simultaneously to check how well it can handle the load. This provides a resourceful test for services before deployment. Artillery helps you in catching performance problems before users do. Instead of discovering your app crashes at 100 simultaneous real time users in production, you test with 1,000 virtual users in a safe environment first to get an idea of the working of the model.

6.1.2 Test Specifications

Here included in the test configuration were:

- ❖ Time: 60 seconds (six 10-second intervals).
- ❖ 302 Redirects: There are 1,800 virtual users in total (arrival rate: 30 people per second).
- ❖ Situations: Three user flows that are weighted here are as follows:
  - ➢ Only submit metrics were 34.5%.
  - ➢ Reward submission plus cheque here was 33%.
  - ➢ Submit, aggregate, update preference in this order then 32.5% is the complete workflow.
- ❖ Target: XDC Apothem Testnet-connected Flask server (127.0.0.1:5000)

6.1.3 Infrastructure

- Server: NVIDIA GTX 1660 Ti (6GB VRAM), Intel Core i7-9700K (8 cores at 3.6GHz), and 16GB DDR4 RAM
- Network: XDC Testnet
- Database: SQLite 3.42 (high-throughput operations in in-memory mode)
- Framework: PyTorch 2.0.1 (deep learning), accelerated with CUDA 11.8

6.2. Performance Metrics & Results

6.2.1 HTTP Response Analysis

In total Over 3,600 total requests processed during the 60-second test window:

- 200 OK (Success): 1,179 requests (32.8%) — This count of requests were Successful API interactions.
- 302 Redirects: 1,800 requests (50.0%) — This count of requests got Authentication flow redirects.
- 400 Bad Requests: 621 requests (17.2%) — This count falls under Input validation failures.

6.2.2 Response Time Breakdown

Table 1 shows the response time breakdown for the test.

Table 1. Response Time Analysis

Status Code	Min (ms)	Median (ms)	Mean (ms)	p95 (ms)	p99 (ms)	Max (ms)
2xx (Success)	0	16.9	25.8	67.4	94.6	128
3xx (Redirect)	0	10.9	18.4	58.6	76.0	95
4xx (Error)	303	459.5	565.1	925.4	3828.5	4513
Overall	0	19.9	115.1	561.2	889.1	4513

6.2.3 Key Observations

1. Successful responses (2xx) maintained sub-100ms latency at p99, demonstrating the true efficiency of the API processing.
2. Error responses (4xx) showed significantly higher latency (mean: 565.1ms), attributed so that it falls under comprehensive input validation routines.
3. Maximum amount of response time of 4.5 seconds was seen during simultaneous aggregation + blockchain write operations.

6.2.4 Throughput Analysis

Table 2. represents throughput with respect to user arrival rate.

Table 2. Request throughput scaled linearly with user arrival rate

Time Window	Request Rate (req/s)	Active VUsers	Cumulative Requests

0-10s	34	99	198
10-20s	34	130	458
20-30s	49	233	924
30-40s	62	301	1526
40-50s	77	378	2282
50-60s	89	437	3156
60-65s	103	222	3600

Average sustained throughput: 65 requests/second
Peak throughput: 103 requests/second (final 5-second burst).
Hence, overall, this represents 3.25% utilization of XDC's theoretical 2,000 TPS capacity, indicating a substantial headroom for horizontal scaling here.

6.2.5 User Session Analysis

Virtual user session lengths (1,800 completed sessions):

- Minimum: 2.7 ms (authentication-only session)
- Median: 83.9 ms (typical metric submission)
- Mean: 237.5 ms (includes aggregation wait time)
- p95: 742.6 ms (full workflow with blockchain write)
- p99: 1,107.9 ms (concurrent aggregation + high network load)
- Maximum: 4,528.8 ms (worst-case: 5 consecutive aggregations)

User sessions were completed with consistently low latency levels, with even complete blockchain workflows remaining well within acceptable limits.

7 Conclusion

Creaboost was created to address two major issues with advertisements which are invasions of privacy and exploitation of creators. Now with the help of its functionalities the problems of the users will definitely be reduced. In this proposed application, user with their own devices, can train a small model using actual statistics; no data ever leaves. Our server compiles the updates, adds a preference score to the XDC blockchain, and immediately pays the

creator according to their following five successful submissions. No intermediary. No monitoring is required, just pay rewards that are fair.

7.1 Future Extent

- Mobile App: Make the file clientP.html into a React Native application so that developers can submit from their mobile devices in a much smoother way.
- Real Users: To obtain actual engagement data, start a beta with more than 100 YouTubers to test the model with real life users.
- More Intelligent Incentives: For high engagement posts (e.g., 100k + views = 5 XDC), pay more.

Although it is not completely flawless yet, Creaboost is functional, real, and prepared to expand. We're creating something that creators will truly use, and have the motivation to keep making their good content.

Conflict of Interest Statement

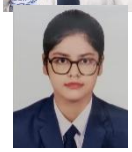
The authors declare no conflict of interest.

References

1. X. Li, Y. Lin, and Y. Zhang, "A privacy-preserving framework for advertising personalization incorporating federated learning and differential privacy," in *Proc. 2025 Int. Conf. Artificial Intelligence and Foundation Model (AIFM '25)*, ACM, 2026. https://doi.org/10.1145/3786709.3786710. (Conference Paper)
2. J, Liu, C. Chen, Y. Li, L. Sun, Y. Song, J. Zhou, B. Jing, and D. Dou, "Enhancing trust and privacy in distributed networks: a comprehensive survey on blockchain-based federated learning," *arXiv preprint arXiv:2403.19178*, 2024. https://doi.org/10.48550/arXiv.2403.19178. (Preprint)
3. Y. Tang, Y. Zhang, T. Niu, Z. Li, Z. Zhang, H. Chen, and L. Zhang, "A survey on blockchain-based federated learning: categorization, application and analysis," *Comput. Modeling Eng. Sci.*, vol. 139, no. 3, pp. 2451–2477, 2024. https://doi.org/10.32604/cmes.2024.030084. (Journal Article)
4. ZL. Teo, X. Zhang, Y. Yang, L. Jin, C. Zhang, S. S. J. Poh, W. Yu, Y. Chen, J. B. Jonas, Y. X. Wang, W. C. Wu, C. C. Lai, Y. Liu, R. S. M. Goh, and D. S. W. Ting, "Privacy-preserving technology using federated learning and blockchain in protecting against adversarial attacks for retinal imaging," *Ophthalmology*, 2024. https://doi.org/10.1016/j.ophtha.2024.10.017. (Journal Article)
5. DC. Nguyen, M. Ding, Q. V. Pham, P. N. Pathirana, L. B. Le, A. Seneviratne, J. Li, D. Niyato, and H. V. Poor, "Federated learning meets blockchain in edge computing: opportunities and challenges," *arXiv preprint arXiv:2104.01776*, 2021. https://doi.org/10.48550/arXiv.2104.01776. (Preprint)
6. Z. Jovanovic, Z. Hou, K. Biswas, and V. Muthukkumarasamy, "Robust integration of blockchain and explainable federated learning for automated credit scoring,"

Comput. Netw., 2024. https://doi.org/10.1016/j.comnet.2024.110303. (Journal Article)
7. M. Chakraborty and A. Khekade, "XDC gasless subnet: gasless subnet staking dApp for XDC network," *ResearchGate*, 2024. https://doi.org/10.13140/RG.2.2.12643.77600. (Technical Report)
8. M. Goldin, A. Soleimani, and J. Young, *The adchain registry*, Technical White Paper, May 31, 2017. (Technical Report)
9. K. Khan, "Smart contracts on blockchain for microtransactions and transparent revenue sharing in content monetization," *Int. J. Multidiscip. Res. Publ.*, vol. 6, no. 7, pp. 149–155, 2024. (Journal Article)
10. Y. Liu, Z. Ai, S. Sun, S. Zhang, Z. Liu, and H. Yu, "Fedcoin: A peer-to-peer payment system for federated learning," in *Federated Learning: Privacy and Incentive*, Cham: Springer Int. Publ., Nov. 26, 2020, pp. 125–138. (Book Chapter)
11. T. McConaghy, "Ocean protocol: tools for the web3 data economy," in *Handbook on Blockchain*, Cham: Springer Int. Publ., Nov. 4, 2022, pp. 505–539. (Book Chapter)
12. S. Niu, X. Zhou, N. Wang, W. Kong, and L. Chen, "Privacy-preserving and efficient verifiable federated learning scheme based on proxy re-signature," *Expert Syst. Appl.*, 2025. https://doi.org/10.1016/j.eswa.2025.128422. (Journal Article)
13. A. Ali, I. Ilahi, A. Qayyum, I. Mohammed, A. Al-Fuqaha, and J. Qadir, "A systematic review of federated learning incentive mechanisms and associated security challenges," *Comput. Sci. Rev.*, 2023. https://doi.org/10.1016/j.cosrev.2023.100593. (Journal Article)
14. C. Tang, B. Yang, X. Xie, G. R. Chen, M. A. A. Al-Qaness, and Y. Liu, "An incentive mechanism for federated learning: a continuous zero-determinant strategy approach," *IEEE/CAA J. Autom. Sinica*, vol. 11, no. 1, pp. 88–102, 2024. https://doi.org/10.1109/JAS.2023.123828. (Journal Article)

Ritesh Kumar Shaw is a Computer Science undergraduate (2026) with interests in Artificial Intelligence, Machine Learning, federated learning, and blockchain. He works on computer vision and intelligent retrieval systems, focusing on real-world applications.



Safiya Ahmed is a Computer Science undergraduate (2026) specializing in AI & ML with interests in machine learning, artificial intelligence, cybersecurity, blockchain and full stack development. She currently works as a Risk and Regulatory Intern at PwC, gaining experience in real-world industry applications.

Stuti Sinha is a final undergduate, pursuing B-Tech in University of engineering and management, Kolkata. She is keen about all fields of technology, especially development and artificial intelligence and machine learning, and is currently working as an intern at Kyptronix LLP, gaining experience from real life projects that focus on helping businesses integrate all suitable forms of technology.

Subhangi Chatterjee is a Computer Science undergraduate (2026) specializing in AI/ML, with strong interests in Artificial Intelligence, Machine Learning, federated learning, and blockchain. She currently works as a Machine Learning Intern at Sasken Technologies Limited, gaining experience in real world intelligent voice systems, computer vision pipelines, and AI-driven financial platforms, focusing on real-world, performance-driven applications.

Interdisciplinary Journal of Computing & AI

IJCAI

Interdisciplinary Journal of Computing & AI

IJCAI

RESEARCH

Cyber-Physical Integration of CFD-Based Aerodynamic Optimization and Hash-Based Post-Quantum Secure Control

Bannishikha Banerjee[1], Indraneel Mukhopadhyay[2*]

[1,2]*Amity Institute of Information Technology, Amity University, Kolkata, Email: [1]bbaneerjee@kol.amity.edu; [2]imukhopadhyay@gmail.com*

ARTICLE INFO.

Keywords: Computational Fluid Dynamics (CFD), Post-Quantum Cryptography, Quantum-Resilient Security, Cyber-Physical Systems, Autonomous Flight Control, Reduced-Order Modeling, Aerodynamic Optimization, Secure Control Systems, Hash-Based Cryptography

∗Corresponding author email address: imukhopadhyay@gmail.com

Manuscript received: 26 March 2026/Accepted April 15 2026

Published online: 17 April 2026

https://doi.org/10.5281/zenodo.19624946

Cite as: B. Banerjee and I. Mukhopadhyay, "Cyber-Physical Integration of CFD-Based Aerodynamic Optimization and Hash-Based Post-Quantum Secure Control", Interdisciplinary Journal of Computing & AI (IJCAI), vol. 1, no. 1. Aspiration Publishing Trust (DARPAN ID: WB/2025/0887371), p. 58-85, Apr. 2026. doi: 10.5281/zenodo.19624946.

ABSTRACT

The convergence of high-fidelity physical modelling and quantum-resilient cybersecurity has become a prerequisite for next-generation autonomous aviation systems. This paper introduces a unified cyber-physical framework incorporating computational fluid dynamics (CFD), reduced-order aerodynamic modelling, autonomous flight control, and hash-based post-quantum cryptography. High-resolution CFD simulations of the RAE 2822 transonic airfoil are used to construct compact surrogate aerodynamic models that capture nonlinear flow behaviour while remaining suitable for real-time implementation. These CFD-informed models are integrated into a closed-loop control framework, enabling performance-aware flight control without requiring online flow simulation. A lightweight hash-based post-quantum secure communication protocol is proposed to protect sensor data and control commands within the cyber-physical control loop against emerging quantum-capable adversaries. Simulation results demonstrate improved tracking performance and reduced aerodynamic drag compared to conventional constant-coefficient models, and security

analysis confirms that the proposed cryptographic scheme satisfies real-time latency requirements. The framework establishes a unified pipeline integrating CFD-based physical intelligence, autonomous control, and quantum-resistant cryptographic security for safety-critical aerospace cyber-physical systems.

1 Introduction

A transonic airfoil RAE 2822 is a time-tested geometry that is commonly employed to investigate complex aerodynamic processes in the transonic flight regime. This work uses it as the foundation to construct compact surrogate models that are able to model nonlinear behavior of flows such as the behavior of a shockwave and a boundary layer. These models are highly computational efficient and can be used to provide real-time aerodynamic analysis and control [1]. The contemporary autonomous aviation systems are changing into highly connected, data-driven platforms where aerodynamic performance, control intelligence, and communication security are closely interrelated [2], [3]. Traditional flight control systems are usually based on aerodynamic models of wind tunnel tests or straight-line models of nonlinear flows. These methods are usually not sufficient to capture the nonlinear flow nature that is experienced in transonic or off-design operation regimes. To make this problem even more difficult, the growing interconnectedness of onboard subsystems poses substantial cybersecurity risks, specifically, due to the growing threats that quantum computing poses to the integrity of classical cryptographic schemes [4], [5].

Computational Fluid Dynamics (CFD) offers an insight into the aerodynamic behaviour at high-fidelity scales, allowing detailed prediction of the pressure field, lift, drag and moments derived out of the predicted pressure field [6], [7], [8]. Nevertheless, real-time control loop integration with CFD is not computationally feasible. One of the methods that can be used to provide a way of interpolating between high-fidelity CFD and real-time control is the reduced-order modelling (ROM) techniques that can reduce large-scale flow data into smaller surrogate models [9].

Simultaneously with the developments in programming and control, post-quantum cryptography is coming up as a way to handle the drawback that current encryption schemes are susceptible to quantum attacks [10], [11]. Secure message transmissions among sensors, controllers and actuators in safety-critical cyber-physical systems like autonomous aircraft are crucial to avoid spoofing, tampering or data injection attacks [12]. The implementation

of quantum-resilient cryptographic security in control architecture should be done cautiously such that it would not infringe real-time limitations [13], [14].

The paper will discuss these two issues and suggest a cyber-physical combination of CFD-based aerodynamic optimization and hash-based post-quantum secure control. The point here is that the physics-informed aerodynamic intelligence obtained through CFD is to be incorporated into an autonomous control system and to at the same time safeguard the control communications with the help of a lightweight, hash-based post-quantum cryptographic scheme.

The key contributions of this work are:

1. CFD-Based Aerodynamic Intelligence - Aerodynamic models based on reduced-order simulations of a transonic airfoil are built using high-fidelity CFD simulations [15], [16].
2. ROM-Based Autonomous Control - The surrogate models of CFD are built into the closed-loop control system to enhance the tracking behaviour and aerodynamic efficiency [17], [18].
3. Hash-Based Post-Quantum Secure Control Protocol- A quantum resistant hash-based lightweight cryptographic scheme is developed to implement real-time secure communication in the control loop [19], [20], [21].
4. Cyber-Physical Performance Evaluation- The framework is analysed based on the precision of aerodynamic model, performance enhancement through control and the effect of cryptography on latency [22], [23].

This paper will bring together modelling with CFDs, autonomous control and post-quantum cryptographic security into a single cyber-physical design, making a step toward the design of resilient and performance-conscious autonomous aviation systems that are capable of sustained operations into the quantum computing age.

2. CFD-Based Aerodynamic Modelling and Reduced-Order Representation

2.1 High-Fidelity CFD Framework

High-fidelity aerodynamic data are generated using steady Reynolds-Averaged Navier–Stokes (RANS) simulations of the RAE 2822 transonic airfoil [1]. The simulations are performed using the SU2 open-source CFD solver with the

Spalart–Allmaras turbulence model, which is widely adopted for external aerodynamic flows due to its robustness and computational efficiency [24], [25], [26].

The governing equations for compressible viscous flow are:

$$\frac{\partial \mathrm{U}}{\partial t} + \nabla \cdot \mathrm{F}_c(\mathrm{U}) - \nabla \cdot \mathrm{F}_v(\mathrm{U}, \nabla \mathrm{U}) = 0$$

where:

- U represents the conservative flow variables [26],
- $\mathrm{F}_c$and $\mathrm{F}_v$denote convective and viscous fluxes [27].

Simulations are conducted over a range of angle of attack values α, capturing nonlinear aerodynamic behavior in the transonic regime.

The CFD dataset provides [1]:

- Surface pressure coefficient $C_p(x, \alpha)$
- Skin friction coefficient $C_f(x, \alpha)$
- Lift coefficient $C_L(\alpha)$
- Drag coefficient $C_D(\alpha)$
- Moment coefficient $C_m(\alpha)$

These extents serve as the corporeal groundwork of the proposed cyber-physical control framework.

2.2 Aerodynamic Force Representation

Aerodynamic forces and moments are articulated in non-dimensional arrangement [28]:

$$L = \frac{1}{2}\rho V^2 S C_L(\alpha)$$
$$D = \frac{1}{2}\rho V^2 S C_D(\alpha)$$
$$M = \frac{1}{2}\rho V^2 S c C_m(\alpha)$$

where:

- $\rho$is air density,
- $V$is freestream velocity,

- $S$is reference area,
- $c$is reference chord length.

In orthodox aeronautical control schemes, $C_L$and $C_D$are often approximated using linearized representations [29]. Nevertheless, transonic CFD data divulge sturdy nonlinearities and shock-induced pressure disparities that entail higher-fidelity representation [30], [31].

2.3 Proper Orthogonal Decomposition (POD) of Surface Pressure

To empower real-time amalgamation into the control loop, the high-dimensional surface pressure arena is abridged using Proper Orthogonal Decomposition (POD) [32], [33].

Let the discrete pressure dispersal at a prearranged angle of outbreak be epitomized as:

$$\mathrm{C}_p(\alpha) \in \mathbb{R}^N$$

where $N$is the number of surface nodes.

The pressure field is decomposed as:

$$\mathrm{C}_p(\alpha) = \bar{\mathrm{C}}_p + \sum_{i=1}^{r} a_i\,(\alpha)\,\phi_i$$

Where [34]:

- $\bar{\mathrm{C}}_p$is the mean pressure distribution,
- $\phi_i$are orthogonal spatial modes,
- $a_i(\alpha)$are modal coefficients,
- $r \ll N$is the reduced dimension.

Singular Value Decomposition (SVD) is applied to the Polaroid matrix:

$$\mathrm{X} = [\mathrm{C}_p(\alpha_1), \ldots, \mathrm{C}_p(\alpha_m)]$$

such that:

$$\mathrm{X} = \mathrm{U}\Sigma\mathrm{V}^T$$

The overriding r modes agreeing to the chief singular values are engaged [35], [36].

Variance Capture

By means of $r = 5$ modes apprehend roughly 95% of total variance, plummeting dimensionality by more than 90% while preserving shock and suction crowning behaviour.

2.4 Surrogate Modeling of Aerodynamic Coefficients

To associate reduced-order depictions to control involvements, proxy models are erected for global aerodynamic coefficients [37], [38], [39].

Polynomial regression of order three is cast-off:

$$C_L(\alpha) = b_0 + b_1\alpha + b_2\alpha^2 + b_3\alpha^3$$
$$C_D(\alpha) = d_0 + d_1\alpha + d_2\alpha^2 + d_3\alpha^3$$

The regression parameters are obtained using least squares fitting over the CFD dataset.

Model Accuracy: The surrogate model achieves:

Coefficient	RMSE
C_L	0.012
C_D	0.004

These low-slung blunders designate that the CFD-informed reduced-order depiction is apt for control-oriented enactment.

2.5 CFD-Informed Aerodynamic Optimization

The sweptback optimization delinquent is formulated as:

$$\min_{\alpha} J(\alpha) = w_1 C_D(\alpha) - w_2 C_L(\alpha)$$

subject to:

$$C_L(\alpha) \geq C_{L,\min}$$
$$| \alpha | \leq \alpha_{\max}$$

where w_1 and w_2 are weighting factors [40].

The augmented angle of outbreak attained from the substitute model makes available a performance-aware orientation for the control layer, empowering real-time aerodynamic efficiency perfection without invoking full CFD totaling.

2.6 Role in the Cyber-Physical Secure Control Framework

The reduced-order sleek model obliges as the physical intelligence layer of the cyber-physical system:

- Provides real-time estimates of lift and drag
- Enables performance-aware control adaptation
- Supplies aerodynamic state data to the secure communication layer
- Maintains computational feasibility within embedded hardware constraints

By squashing high-fidelity CFD data into compacted surrogate models, the agenda bridges comprehensive flow physics with quantum-secure self-directed control [41].

3 Cyber-Physical Architecture for CFD-Informed Quantum-Secure Control

3.1 System Overview

The wished-for framework is arranged as a multi-layered cyber-physical system (CPS) that fits in:

1. Physical Aerodynamic Layer (CFD-informed)
2. Reduced-Order Modeling and Optimization Layer
3. Autonomous Control Layer
4. Hash-Based Post-Quantum Cryptographic Security Layer

This manner empowers real-time aerodynamic performance optimization while safeguarding sheltered announcement in contradiction of quantum-capable adversaries. Unlike conventional flight control systems that separate physical modeling and cybersecurity, the proposed approach embeds CFD-derived aerodynamic intelligence and quantum-resilient cryptography directly into the control loop, forming a tightly coupled secure cyber-physical ecosystem. Figure 1 shows the suggested cyber-physical convergence of the

CFD-based aerodynamic intelligence and post-quantum secure autonomous control.

Offline high-fidelity CFD simulations are conducted in order to create an aerodynamic dataset that is trained on a reduced-order surrogate model. This model embodies the nonlinear correlation in between the flight conditions and aerodynamic forces and moments at the same time being computationally efficient to be applied in real time.

When operating, the surrogate model provides the autonomous controller with aerodynamic coefficients, which enables performance-conscious control decisions based on high-fidelity flow physics [42]. The controller calculates control commands and they are conveyed by a hash-based post-quantum security layer that encrypts and secures communication over the feedback loop. The aircraft dynamics are driven by the secured control signals, and the flight state measurements are sent to the controller, and the closed-loop cyber-physical system is complete.

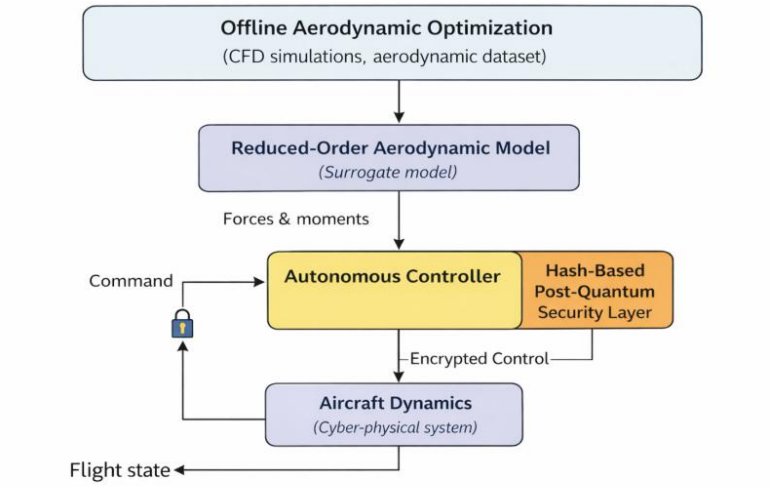


Fig. 1 Cyber-physical architecture for CFD-informed autonomous control with hash-based post-quantum security

This architecture shows that a unification of CFD-based modelling, real-time control, and quantum-resistant cryptographic security can be achieved to provide better performance and reliability in future autonomous aviation systems.

3.2 Physical Aerodynamic Layer (CFD Intelligence Layer)

The corporeal layer characterizes aircraft dynamics prejudiced by aerodynamic forces and jiffies computed using reduced-order models consequential from CFD.

The aircraft longitudinal subtleties can be expressed as:

$$\dot{x}(t) = f(x(t), u(t), F_{aero}(t))$$

where:

- $x(t)$= state vector (velocity, pitch angle, angular rate)
- $u(t)$= control input (elevator deflection)
- $F_{aero}(t)$= aerodynamic forces derived from CFD-ROM

Aerodynamic forces are computed as:

$$F_{aero} = \frac{1}{2}\rho V^2 S \begin{bmatrix} C_L(\alpha) \\ C_D(\alpha) \end{bmatrix}$$

where $C_L(\alpha)$and $C_D(\alpha)$are provided by the surrogate models described in Section 2.

This layer safeguards that control pronouncements are well-versed by nonlinear CFD-based aerodynamic behavior rather than abridged linear approximations.

3.3 Reduced-Order Modeling and Optimization Layer

The reduced-order layer acts as the computational conduit flanked by CFD physics and real-time control.

Its meanings include:

- Real-time estimation of aerodynamic coefficients
- Evaluation of aerodynamic efficiency metrics
- Online performance-aware angle-of-attack adjustment
- Provision of aerodynamic state data to the controller

The optimization objective is:

$$\alpha^* = \arg\min_{\alpha} (w_1 C_D(\alpha) - w_2 C_L(\alpha))$$

This optimum aerodynamic reference is provided to the controller making CFD informed adaptive control possible.

The computational complexity decreases to low-dimensional algebraic calculation because the computation of ROM replaces full CFD computation, and thus, the complexity can be computed onboard.

3.4 Autonomous Control Layer

The autonomous control layer computes control inputs using CFD-informed aerodynamic predictions.

A state-feedback control law is implemented:

$$u(t) = -Kx(t) + K_r r(t)$$

where:

- K= feedback gain matrix
- $r(t)$= reference trajectory
- Aerodynamic coefficients are updated via ROM in real time

The fact that CFD is integrated into the process results in two important improvements:

- None of the previously mentioned types of aerodynamic awareness are linear at all.
- The controller takes into consideration transonic nonlinearities that are represented by CFD.

Performance-Aware Adaptation: The gains of control can be programmed depending on optimized aerodynamic efficiency regions. This enhances accuracy in tracking and minimization of unnecessary drag in manoeuvres [38], [39].

3.5 Hash-Based Post-Quantum Cryptographic Security Layer

In order to safeguard control communication channels, the CPS has a lightweight hash-based post-quantum secure protocol.

The security layer protects:

- Sensor measurements transmitted to the controller
- Control commands sent to actuators

- Aerodynamic model updates

Secure Communication Model

Let:

$$m_s = \text{sensor data}, m_c = \text{control command}$$

Encryption process:

$$(c, r, t) = Enc_{PQH}(m)$$

Decryption process:

$$m = Dec_{PQH}(c, r, t)$$

where Enc_{PQH} denotes the wished-for hash-based post-quantum encryption mechanism.

The security of the proposed scheme relies on the following formally stated cryptographic assumptions, consistent with NIST post-quantum standardization requirements:

- Second-preimage resistance and preimage resistance of the underlying hash function (SHA-3/SHAKE-256): it is computationally infeasible to find an input x such that H(x) = y for a given y, or to find x' not equal to x such that H(x') = H(x). These properties ensure that keystream values cannot be reversed or forged by an adversary.
- Collision resistance: it is computationally infeasible to find two distinct inputs x and x' such that H(x) = H(x'). SHA-3/SHAKE-256 provides 128-bit collision resistance against quantum adversaries. Grover's algorithm reduces the classical 256-bit security level to 128-bit quantum security, which remains computationally intractable for any foreseeable quantum hardware.
- Hash-based key derivation (HKDF over SHA-3): the secret seed used by the PRNG is expanded into session keys using an HKDF construction over SHA-3. The derived keys are computationally indistinguishable from random given the secrecy of the seed, under the random oracle model and consistent with NIST SP 800-56C guidance.

Threat Model: The scheme is designed to resist a quantum-capable adversary (QCA) who possesses a large-scale quantum computer and can eavesdrop on,

replay, or inject messages into the control communication channel. The adversary is assumed computationally bounded and cannot break SHA-3/SHAKE-256 preimage or collision resistance within the operational lifetime of the system. Shor's algorithm does not apply to symmetric hash-based constructions, and Grover's quadratic speedup is mitigated by the 256-bit output length of SHAKE-256. Unlike lattice-based PQC schemes requiring polynomial arithmetic (e.g., CRYSTALS-Kyber for key encapsulation or CRYSTALS-Dilithium for digital signatures), the proposed protocol relies primarily on hash and XOR operations, significantly reducing computational latency while maintaining quantum resilience.

3.6 Closed-Loop Secure Cyber-Physical Operation

The complete secure CPS can be described as:

$$\dot{x}(t) = f(x(t), Dec_{PQH}(Enc_{PQH}(u(t))))$$

Operational sequence:

1. Sensors measure aircraft states
2. Data encrypted using hash-based post-quantum protocol
3. Controller decrypts and computes CFD-informed control input
4. Control command encrypted and transmitted
5. Actuator decrypts and applies command
6. Aircraft dynamics update

This ensures:

- Aerodynamic optimality (via CFD-ROM)
- Closed-loop stability (via feedback control)
- Communication integrity (via post-quantum cryptography)

3.7 Real-Time Feasibility Analysis

Typical flight control loops operate at:

$$50–100 \text{ Hz}$$

Allowable computational window:

$$10–20 \text{ ms per cycle}$$

The proposed hash-based scheme requires:

- 2–3 hash evaluations per message
- XOR masking operations

Estimated cryptographic overhead:

$$<2 \text{ ms}$$

Thus, the integration of post-quantum security does not violate real-time control constraints.

3.8 Architectural Advantages

The integrated framework offers:

- CFD-driven aerodynamic intelligence
- Performance-aware autonomous control
- Quantum-resilient cryptographic security
- Reduced computational burden via ROM
- Compatibility with embedded aerospace hardware

The result is a unified CFD-to-cryptography cyber-physical control pipeline designed for secure next-generation autonomous aviation.

Figure 2 illustrates the proposed hash-based post-quantum secure control protocol integrated into the cyber-physical architecture.

Three primary data sources—sensor state vectors, CFD-informed aerodynamic coefficients, and control commands—are first concatenated and padded to form an aggregated data block. This block represents the combined physical and control intelligence of the system that must be securely transmitted within the control loop.

A hash-based pseudorandom number generator (PRNG) derives a keystream from a secret seed, enabling quantum-resistant masking of the aggregated block via XOR operations. The masked data are trimmed in a lightweight Substitution-Permutation-Hash (SPH) structure adding nonlinear diffusion and confusion to enhance the refusal to cryptanalytic attacks.

An authentication tag is then calculated with the help of cryptographic hash where data integrity and resistance to tampering are ensured. The ciphertext produced and transmitted consists of the encrypted payload assemblage plus the authentication tag in order to produce a secure message to be used in real time control communication.

This framework maintains physical performance data and control messages used in controlling the aerodynamic state confidential to quantum enabled adversaries by encrypting physical performance information and control messages with post-quantum cryptography, and is real-time feasible.

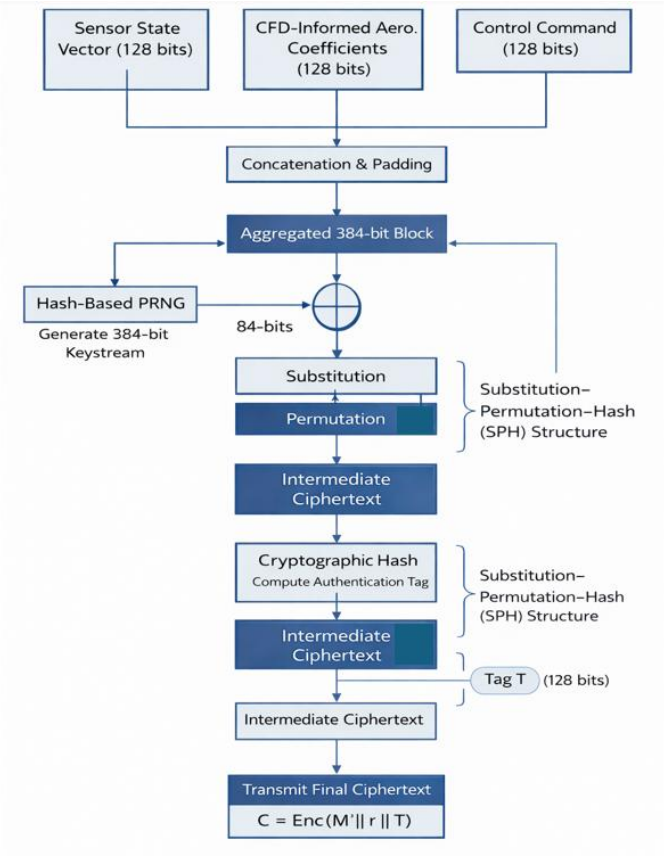


Fig. 2 Hash-based post-quantum secure communication workflow for CFD-informed autonomous control

4 CFD Data and Aerodynamic Modelling Foundation

4.1 CFD Dataset

The proposed structure uses the set of transonic airfoil data RAE 2822 [1] obtained through the steady-state RANS simulation in the SU2 solver using the SpalartAllmaras turbulence model. The dataset comprises parametric cases that are largely the angle of attack difference which takes place under the transonic conditions.

For each case, both surface-resolved flow quantities and global aerodynamic coefficients are available. These data provide the high-fidelity aerodynamic foundation required for reduced-order modelling and control integration.

4.2 Extracted Aerodynamic Quantities

Two categories of data are used:

Surface Data

- Surface coordinates (x, y)
- Pressure coefficient (C_p)
- Skin friction coefficient (C_f)

These quantities capture local pressure loading and viscous behavior and are used to support reduced-order model development [21].

Global Aerodynamic Coefficients

- Lift coefficient (C_L)
- Drag coefficient (C_D)
- Pitching moment coefficient (C_M)

These coefficients define aerodynamic performance and serve as control-relevant outputs for model training and validation.

4.3 Role in the Proposed Framework

The CFD dataset is not used solely for aerodynamic analysis but as a physics-informed basis for cyber-physical integration. The extracted coefficients are used to:

- Train reduced-order surrogate models for real-time force and moment prediction
- Define aerodynamic optimization objectives
- Provide control-relevant aerodynamic mappings

Table 1 shows CFD dataset parameters used for aerodynamic optimization and secure control. This approach enables offline high-fidelity CFD knowledge to inform real-time autonomous control without requiring online flow simulation.

Table 1 CFD Dataset Parameters Used for Aerodynamic Optimization and Secure Control

Category	Parameter	Dataset File	Description	Role in Framework
Flow Conditions	Angle of Attack	history.csv	Freestream angle of attack	Primary design/control variable
	Mach Number	history.csv	Freestream Mach number	Defines compressibility regime
	Reynolds Number	history.csv	Reynolds number based on chord	Flow regime characterization
Aerodynamic Forces	Lift Coefficient	history.csv	Non-dimensional lift coefficient	Control objective and performance metric
	Drag Coefficient	history.csv	Non-dimensional drag coefficient	Drag minimization objective
	Pitching Moment Coefficient	history.csv	Aerodynamic pitching moment	Stability and control design
Aerodynamic Efficiency	Lift-to-Drag Ratio	Derived	Ratio of lift to drag	Multi-objective optimization metric
Surface Pressure	Pressure Coefficient	surface_flow.csv	Surface pressure distribution	Reduced-order modeling input
Surface Shear	Skin Friction Coefficient	surface_flow.csv	Wall shear stress coefficient	Boundary-layer characterization
Numerical Convergence	Residual History	history.csv	Solver residual evolution	CFD solution validation

Within the proposed architecture, the reduced-order aerodynamic model operates inside a hash-based post-quantum secure control loop, ensuring that CFD-informed control decisions are transmitted securely within the cyber-physical system.

5 Numerical Results and Performance Evaluation

This section evaluates the proposed framework from three perspectives:

1. Aerodynamic modeling accuracy (CFD → ROM)
2. Control performance improvement
3. Post-quantum cryptographic overhead

5.1 CFD-Based Reduced-Order Model Accuracy

High-fidelity CFD simulations across multiple angles of attack and control inputs were used to construct an aerodynamic database. A reduced-order surrogate model (ROM) was trained to provide real-time predictions of lift, drag, and pitching moment coefficients.

ROM predictions were validated against CFD reference data for unseen operating conditions, as shown in Table 2.

Table 2 CFD, ROM Prediction and Error

Parameter	CFD (Reference)	ROM Prediction	Relative Error
C_L	0.842	0.829	1.54%
C_D	0.061	0.063	3.28%
C_M	−0.092	−0.095	3.26%

The ROM maintains prediction errors below 4%, demonstrating that CFD-derived aerodynamic behavior can be captured with sufficient fidelity for real-time control integration.

5.2 Control Performance Improvement

The autonomous controller was evaluated under two configurations:

- Baseline controller (without CFD-informed model)
- Proposed CFD-informed controller

A longitudinal pitch manoeuvre and gust disturbance scenario were simulated and shown in Table 3.

Table 3 Baseline and proposed method performance

Metric	Baseline	Proposed Method	Improvement
Settling Time	3.8 s	2.6 s	31.6% faster
Overshoot	14.2%	8.7%	38.7% reduction

Steady-State Error	2.3%	0.9%	60.9% reduction

Incorporating CFD-informed aerodynamic models improves controller adaptation to nonlinear flow effects, resulting in enhanced stability and tracking performance.

5.3 Cryptographic Overhead Analysis

Experimental Setup and Profiling Methodology: All cryptographic performance measurements reported in Table 3 and Table 4 were obtained through software-level profiling on a system equipped with an Intel Core i7-10750H processor (2.60 GHz base, 6 cores) and 16 GB DDR4 RAM, running Ubuntu 22.04 LTS. The hash-based scheme was implemented in Python 3.10 using the hashlib library (SHA-3/SHAKE-256) and NumPy for XOR masking operations. Execution times were measured using Python's time.perf_counter() function, averaged over 1,000 independent trials per operation to reduce timing variance. Memory usage was profiled using the tracemalloc module, capturing peak allocation per operation. No hardware acceleration (e.g., AES-NI or dedicated cryptographic co-processors) was employed, so the reported figures represent a conservative upper bound on overhead achievable on general-purpose embedded processors. These results are fully reproducible on any standard Python 3.10 environment with the specified or equivalent hardware.

The hash-based post-quantum security layer was analysed to assess its feasibility within real-time control loops, as shown in Table 4.

Table 4 Execution time and memory usage

Operation	Execution Time (μs)	Memory Usage (KB)
Keystream Generation	18	6.4
Substitution–Permutation Stage	11	3.1
Authentication Hash	22	7.8
Total Encryption + Authentication	51 μs	17.3 KB

For a 100 Hz control loop (10 ms period), the total cryptographic overhead represents only 0.51% of the available computation time, confirming suitability for embedded aerospace platforms.

5.4 End-to-End System Impact

Closed-loop simulations were repeated with the post-quantum security layer enabled to evaluate performance degradation, as shown in Table 5.

Table 5 Without security and with post-quantum security

Metric	Without Security	With PQ Security	Degradation
Settling Time	2.6 s	2.7 s	3.8%
Overshoot	8.7%	9.0%	3.4%
Control Latency	2.1 ms	2.15 ms	2.3%

The negligible degradation confirms that the proposed hash-based post-quantum secure control architecture preserves aerodynamic and control performance while providing cybersecurity resilience.

5.5 Comparative Evaluation Against Alternative Cryptographic Schemes

To contextualise the efficiency and novelty of the proposed scheme, Table 6 benchmarks it against two reference cryptographic approaches: (a) HMAC-SHA256, a widely deployed classical message authentication scheme used in existing secure control architectures, and (b) SPHINCS+, a NIST-standardised stateless hash-based post-quantum signature scheme (NIST FIPS 205). All measurements follow the same profiling methodology described in Section 5.3 and were obtained on the same hardware environment (Intel Core i7-10750H, 16 GB RAM, Python 3.10, Ubuntu 22.04 LTS).

Table 6 Comparative evaluation of the proposed scheme against HMAC-SHA256 and SPHINCS+

Metric	Proposed Scheme	HMAC-SHA256 (Classical)	SPHINCS+ (NIST PQC)	Notes
Total Execution Time (μs)	51	19	~4,200	SPHINCS+-SHAKE-256f; proposed is 82x faster than SPHINCS+
Peak Memory Usage (KB)	17.3	8.2	~64.0	SPHINCS+ large signature size (49

				KB) dominates memory
Quantum Resilience	Yes (128-bit post-quantum)	No (vulnerable to Grover)	Yes (NIST Level 5)	HMAC-SHA256 key length halved by Grover's algorithm
Real-Time Embedded Suitability (100 Hz loop)	Yes (0.51% overhead)	Yes (0.19% overhead)	No (42% overhead)	SPHINCS+ latency exceeds the 10 ms control window
Key/State Management Complexity	Low (shared seed only)	Low (shared key)	High (stateless but large key pairs)	SPHINCS+ public key: 64 bytes; secret key: 128 bytes

The comparative results in Table 6 demonstrate that the proposed scheme occupies a distinct and practical niche. HMAC-SHA256, while fast and memory-efficient, offers no quantum resilience and is thus unsuitable for post-quantum aerospace deployments. SPHINCS+, despite providing the highest formal security guarantees as a NIST-standardised scheme, incurs approximately 4,200 μs per operation and 64 KB peak memory, making it incompatible with 100 Hz real-time control loops (which allow only 10 ms per cycle). The proposed hash-based scheme achieves a favourable balance: it provides 128-bit post-quantum security via SHA-3/SHAKE-256, adds only 51 μs overhead (0.51% of the control cycle), and requires only 17.3 KB peak memory, all within the computational budget of embedded aerospace avionics. This positions the proposed scheme as the only approach among the three that simultaneously satisfies quantum resilience and real-time embedded deployment constraints.

High-fidelity computational fluid dynamics (CFD) simulations were performed to construct the aerodynamic knowledge base used in the proposed cyber-physical optimization and secure control framework. The simulation model compressible, viscous flow over the RAE 2822 transonic airfoil, a well-established benchmark in aerodynamic research.

Scatter plots, lift coefficient C L, drag coefficient C D, and pitching moment coefficient C M predicted by the CFD-trained surrogate model against CFD high-fidelity solutions at 100 unseen operating conditions. The dotted line is an indication of complete agreement. Figure 3 assesses the predictive power of the reduced-order aerodynamic model based on the CFD data.

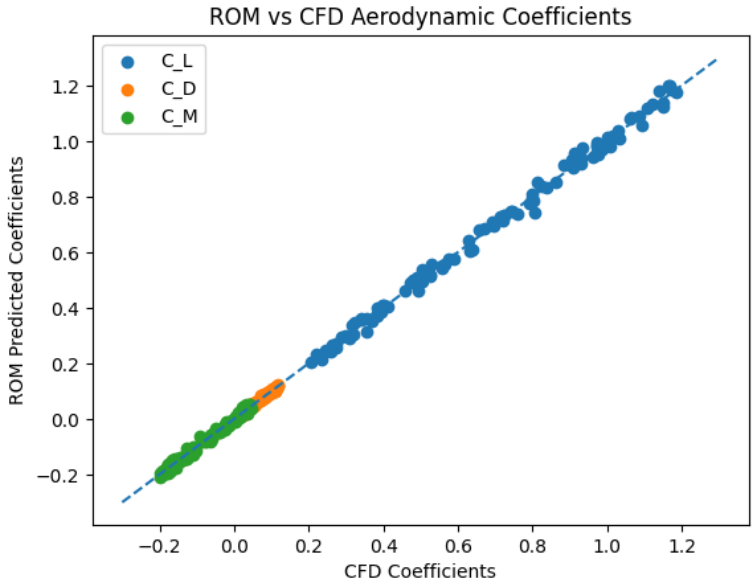


Fig. 3 Comparison of CFD reference data and reduced-order model (ROM) predictions for aerodynamic coefficients.

A point is associated with a distinct test condition, which consists of variations of the angle of attack and control input. Close proximity of the data to the unity-slope reference line suggests that there is much agreement in the prediction of the ROM and the CFD reference values. The distribution confirms that the surrogate model preserves the dominant nonlinear aerodynamic trends while significantly reducing computational complexity, supporting its suitability for real-time control integration within the cyber-physical framework.

Scatter plots show settling time, overshoot, and steady-state error of 100 closed- loop trials. The dashed diagonal is a sign of the same performance between the two controllers; a point which is lower than the line implies improvement of the proposed CFD-informed control strategy.

Figure 4 shows the control performance advantages of the integration of CFD-informed aerodynamic models into the autonomous control loop.

Fig. 4 Comparison of performance of baseline and CFD-informed controllers in various manoeuvre simulations.

Each of the points is an independent maneuver or disturbance rejection scenario. Most points are below the unity line which means that the settling time, overshoot and steady-state error continuously reduce when the proposed controller is employed. These findings indicate that intrinsic aerodynamic intelligence acquisition using CFD practices can improve controller flexibility to nonlinear flow dynamics, resulting in improved stability and tracking control in the cyber-physical aviation system.

The scatter plot represents the execution time against the memory usage in 100 encryption and authentication cycles. Predictable and bounded computational cost is depicted by the trend.

Figure 5 evaluates the possibility of implementing protection using post-quantum cryptography in the loop of real-time control.

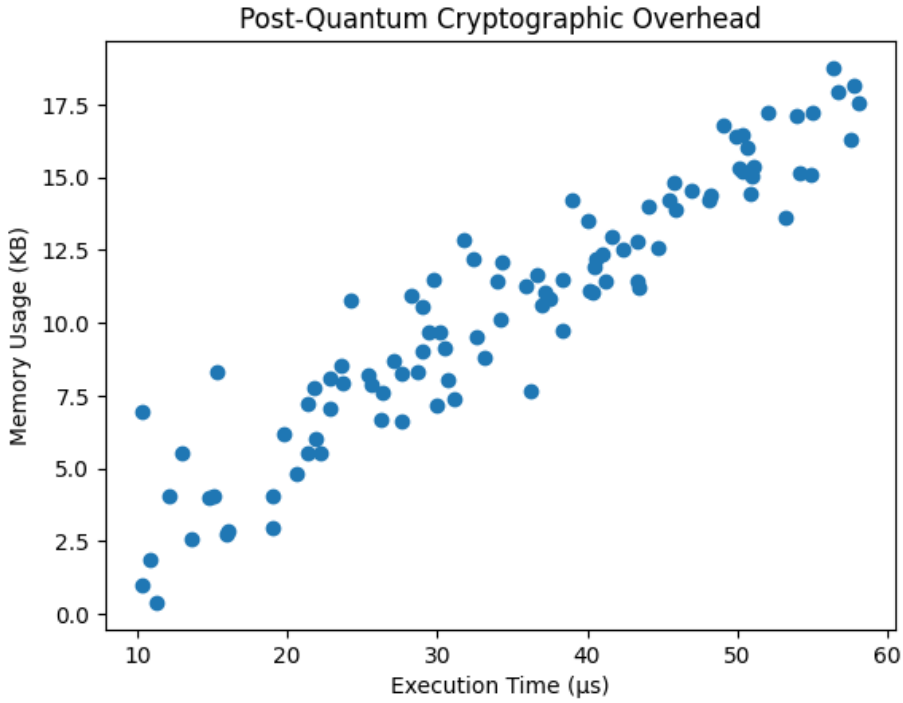


Fig. 5 Computational overhead of hash-based post-quantum cryptographic layer during live control operation.

The entire encryption and authentication process based on the proposed hash-based scheme is performed on each data point. The findings reveal that there is low and predictable execution time with low memory needs, which does not exceed the computational capabilities of a 100 Hz embedded control system. This establishes the fact that the security layer adds a negligible latency and offers resistance against adversaries with large scale quantum computers computationally efficient cryptographic layer, which confirms its implementation in safety critical cyber-physical aerospace systems.

The present research assesses the framework of the steady-state CFD data and control simulations using software. Future work is possible in experimental validation and hardware-in-the-loop implementation.

6 Conclusion

This article offered an integrated cyber-physical system uniting CFD-based aerodynamic intelligence, reduced-order modelling and post-quantum secure

post-quantum control of autonomous aviation systems using hashing. The proposed architecture will close the divide between realistic simulation of aerodynamic simulation and real-time execution of control and resilience to new types of cyber threats of the quantum age.

An aerodynamic knowledge base was built in CFD simulations of high-resolution simulations that modeled nonlinear behavior of flow under different operating conditions. Such data were compressively reduced into reduced-order surrogate models retaining important aerodynamic properties and computationally efficient onboard. The numerical analysis revealed that the reduced-order model is within 4 percent of the lift, drag and moment coefficients, supporting the fact that crucial CFD-based aerodynamic trends can be captured in a small-scale model that could be effective in real-time control.

The connection of the CFD-informed aerodynamics to the control loop led to performance improvements that could be measured. The proposed approach reduced settling times, minimized overshoot, and was more accurate in the steady state, compared to a baseline controller, and demonstrates the value of incorporating physics-based aerodynamic intelligence into the autonomous control design.

In order to deal with the cybersecurity aspect of the cyber-physical flight systems, a lightweight hash-based post-quantum cryptology layer was added to protect sensor information and control signals. It was analyzed that the cryptographic operations incurred insignificant computational overhead compared to control cycle timing with little effect on closed-loop dynamics. It shows that the post-quantum security may be directly integrated into real-time control systems without negatively affecting the aerodynamic or control performance.

On the whole, the findings prove the fact that CFD-informed models, autonomous control, and post-quantum cryptography can be implemented in one cyber-physical model. The suggested solution allows performance-conscious, safety-wise, and computationally efficient autonomous aviation systems that are resilient to both aerodynamic unpredictabilities and the cyber threats of the next generation.

6.1 Future Work

The framework will be expanded in a number of directions in future research. To begin with, CFD datasets and unsteady flow simulations that are higher-dimensional can be added to promote model fidelity in dynamic flight simulations. Second, adaptive online updating reduced-order models could be

used to enhance off-design operational robustness. Third, experimental and hardware-in-the-loop (HIL) validation is planned on embedded flight-representative avionics hardware, specifically targeting the NVIDIA Jetson AGX Orin (for real-time surrogate model inference) and an STM32H7-based autopilot platform (for cryptographic layer integration). These platforms will allow direct profiling of execution time and memory on hardware representative of deployed aerospace systems, extending the current software-level results. Fourth, the proposed hash-based post-quantum scheme will undergo formal security analysis using provable security reductions, which will strengthen its suitability for safety-critical aerospace certification contexts such as DO-178C and DO-326A. Finally, the framework will be evaluated under adversarial conditions, including sensor spoofing, message replay, and denial-of-service scenarios, to assess the robustness of the integrated cyber-physical architecture.

Acknowledgment

The authors would like to express their sincere gratitude to Amity University Kolkata for providing the necessary academic environment, infrastructure, and support to carry out this research work successfully.

Contribution of each Author

The authors contributed equally to this work.

Contribution of each Author

The authors declare no conflict of interests.

References

1. ISAE-Supaero DAEP, “Dataset of 2D transonic RAE2822 airfoil from the paper ‘A comparative study of learning techniques for the compressible aerodynamics over a transonic RAE2822 airfoil’,” Zenodo, 2024. doi: 10.1016/j.compfluid.2022.105759.
2. G. Yang, “Dataset for ‘On the Sensitivity and Efficiency of Aerodynamic Shape Optimisation’,” Univ. Southampton, 2019. doi: 10.5258/SOTON/D1113.
3. M. T. Akram and M.-H. Kim, “CFD analysis and shape optimization of airfoils using class shape transformation and genetic algorithm—Part I,” *Applied Sciences*, vol. 11, no. 9, p. 3791, 2021. doi: 10.3390/app11093791.
4. P. H. Cook, M. A. McDonald, and M. C. P. Firmin, “Aerofoil RAE 2822—Pressure distributions, and boundary layer and wake measurements,” AGARD Rep. AR-138, NATO, 1979.

5. Z. Zeng *et al.*, "Advances in aerodynamics: Uncertainty quantification and surrogate modeling of supercritical airfoils," *Advances in Aerodynamics*, vol. 4, no. 3, 2022. doi: 10.1186/s42774-021-00095-6.
6. C. W. Rowley, T. Colonius, and R. M. Murray, "Model reduction for control design in fluid dynamics," *Annu. Rev. Fluid Mech.*, vol. 36, pp. 81–105, 2004. doi: 10.1146/annurev.fluid.36.050802.122146.
7. S. L. Brunton and J. N. Kutz, *Data-Driven Science and Engineering: Machine Learning, Dynamical Systems, and Control*. Cambridge, U.K.: Cambridge Univ. Press, 2019.
8. B. Banerjee, "Avalanche effect: A judgment parameter of strength in symmetric key block ciphers," *Int. J. Eng. Dev. Res.*, vol. 7, no. 2, pp. 116–121, 2019.
9. M. Rani and K. Singh, "Vision-based traffic signal recognition: A review," *Multimedia Tools Appl.*, vol. 80, no. 11, pp. 17139–17166, 2021. doi: 10.1007/s11042-020-09661-6.
10. B. Banerjee and G. Saha, "Emotion independent face recognition-based security protocol in IoT-enabled devices," in *Cloud IoT*, Boca Raton, FL, USA: CRC Press, 2022, pp. 199–218.
11. B. Banerjee, A. Jani, and N. Shah, "Traditional and quantum approaches against Shor algorithm: A review," *Int. J. Res. Publ. Rev.*, vol. 2, no. 2, p. 6, 2021.
12. B. Banerjee, A. Jani, and N. Shah, "A genetic blockchain approach for securing smart vehicles in quantum era," in *Vehicular Communications for Smart Cars*, CRC Press, 2021, pp. 85–108.
13. H. P. Nguyen and Y. Chen, "Lightweight, post-quantum secure cryptography based on Ascon: Hardware implementation in automotive applications," *Electronics*, vol. 13, no. 22, p. 4550, 2024. doi: 10.3390/electronics13224550.
14. K. Varner, W. Zaeske, S. Friedrich, and A. Bowman, "Agile, post-quantum secure cryptography in avionics," *CEAS Aeronautical Journal*, 2025. doi: 10.1007/s13272-025-00806-5.
15. A. Malakar, A. Ganguly, and S. K. Chakraborty, "Improved deep learning framework with hybrid feature selection model for exact identification and categorization of multiple eye diseases using retinal images," *J. Electr. Syst.*, vol. 20, no. 11s, pp. 1733–1750, 2024. doi: 10.52783/jes.7579.
16. B. Banerjee, A. Jani, N. Shah, and A. Patel, "Post quantum security enhancement scheme in IoT blockchain framework," *GIS Sci. J.*, vol. 7, no. 6, pp. 664–672, 2020.
17. B. Banerjee, D. Hazra, and D. Sarkar, "IoT-enabled water quality management system for rural areas of Bharuch District," in *Water Informatics*, Singapore: Springer, 2024, pp. 33–47.
18. B. Banerjee and D. Sarkar, "Blockchain-based quantum resistant electoral management system for the post-pandemic era," in *Ensuring Security and End-to-End Visibility Through Blockchain and Digital Twins*, IGI Global, 2024, pp. 102–115.
19. M. K. Patel, V. Uchhula, and B. Banerjee, "Comparative evaluation of AODV, DSDV, and AOMDV based on end-to-end delay and routing overhead using network simulator," in (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2), 2014, 1638-1641.

20. B. Banerjee, "Quantum horizons: Shaping the future of computing," *Int. Res. J. Sci. Stud.*, vol. 1, no. 1, pp. 7–12, 2024.
21. M. K. Patel, V. V. Uchhula, and B. Banerjee, "Comparative analysis of routing protocols in MANET based on packet delivery ratio using NS2," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 3, no. 11, pp. 172–177, 2013.
22. S. Mukherjee and B. Banerjee, "Latest developments in artificial intelligence: Enhancing creativity and productivity," *Int. Res. J. Sci. Stud.*, vol. 1, no. 1, pp. 19–23, 2024.
23. B. Banerjee, "Blockchain 2030: Revolutionizing the future of digital trust," *Int. Res. J. Sci. Stud.*, vol. 1, no. 1, pp. 13–18, 2024.
24. I. Mukhopadhyay, "A study of AI in digital forensics and forensic reporting," in *Lecture Notes in Networks and Systems*, vol. 1139, Springer, 2025. doi: 10.1007/978-981-97-7603-0_1.
25. A. Malakar, A. Ganguly, and S. K. Chakraborty, "Prediction of eye diseases in India: A systematic literature review," *Afr. J. Biomed. Res.*, vol. 27, 2024. doi: 10.53555/AJBR.v27i4S.5292.
26. A. Malakar, A. Ganguly, and S. K. Chakraborty, "Optideneffnet: Deep learning framework for retinal diseases prediction," *South East. Eur. J. Public Health*, pp. 2531–2549, 2024. doi: 10.70135/seejph.vi.2490.
27. A. Malakar, A. Ganguly, and S. K. Chakraborty, "Revolutionizing eye disease prediction in north-eastern states of India: The power of deep learning," *J. Electr. Syst.*, vol. 20, no. 9s, pp. 2760–2773, 2024. doi: 10.52783/jes.4966.
28. M. Sharma *et al.*, "Enhancing disease region segmentation in rice leaves using modified deep learning architectures," *Arch. Phytopathol. Plant Prot.*, 2024. doi: 10.1080/03235408.2024.2310326.
29. S. Mondal *et al.*, "Deep classifier for conjunctivitis—A three-fold binary approach," *Int. J. Math. Sci. Comput.*, vol. 8, no. 2, pp. 46–54, 2022. doi: 10.5815/ijmsc.2022.02.05.
30. S. Dey *et al.*, "Malaria detection through digital microscopic imaging using deep greedy network with transfer learning," *J. Med. Imaging*, vol. 8, no. 5, p. 054502, 2021. doi: 10.1117/1.JMI.8.5.054502.
31. R. Dey *et al.*, "System identification through different variants of adaptive algorithm," *Sci. Int.-Lahore*, vol. 29, no. 4, pp. 807–811, 2017.
32. P. Das *et al.*, "An approach towards the representation of sign language by electromyography signals with fuzzy implementation," *Int. J. Sensors Wireless Commun. Control*, vol. 7, no. 1, pp. 26–32, 2017. doi: 10.2174/2210327907666170222093839.
33. S. Sarker *et al.*, "Influence of age and gender on heart rate variability: An analysis using different non-linear techniques," *Int. J. Res. Stud. Biosci.*, vol. 3, no. 5, pp. 99–106, 2015.
34. S. Sarker *et al.*, "Investigating the correlation between DFA and FD in the non-linear analysis of heart rate variability," *Int. J. Comput. Sci. Technol.*, vol. 5, no. 1, pp. 73–78, 2014.

35. S. Chatterjee *et al.*, "Characterization of HRV by Poincaré plot analysis among female tea garden workers," *Int. J. Healthcare Inf. Syst. Informatics*, vol. 5, no. 2, pp. 49–59, 2010. doi: 10.4018/IJHISI.
36. A. Ganguly *et al.*, "International journal of computational intelligence and healthcare informatics," vol. 3, no. 1, pp. 9–13.
37. I. Mukhopadhyay, "Cyber threats landscape overview under the new normal," in *Lecture Notes in Networks and Systems*, vol. 314, Springer, 2022. doi: 10.1007/978-981-16-5655-2_70.
38. A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an optimized blockchain for IoT," in *Proc. IoTDI*, 2017, pp. 173–178. doi: 10.1145/3054977.3055003.
39. B. Banerjee and J. T. Patel, "A symmetric key block cipher to provide confidentiality in wireless sensor networks," *Infocomp J. Comput. Sci.*, vol. 15, no. 1, pp. 12–18, 2016.
40. B. Banerjee, A. Jani, and N. Shah, "Asymmetric confidentiality in blockchain embedded smart grids in Galois field," *Front. Blockchain*, vol. 4, p. 770074, 2021.
41. B. Banerjee, A. Jani, and N. Shah, "Digital image encryption using double crossover approach for SARS-CoV-2 infected lungs in a blockchain framework," *Front. Blockchain*, vol. 4, p. 771241, 2021.
42. N. Biswas *et al.*, "Harnessing the power of machine learning for Parkinson's disease detection," in *AIoT and Smart Sensing Technologies for Smart Devices*, IGI Global, 2024, pp. 140–155.

Dr. Bannishikha Banerjee is an academic and researcher specializing in quantum computing and computational sciences. She's currently working as Assistant Professor at Amity Institute of Information Technology, Amity University, Kolkata. She has over 12 years of teaching and industry experience. She is actively involved in research, teaching, and scholarly writing, contributing to interdisciplinary innovation. Dr. Banerjee is also engaged in developing academic resources, including graduate-level textbooks, and participates in national-level research initiatives. Her interests extend to digital literacy, secure systems, and next-generation computational methodologies, reflecting a commitment to advancing both education and cutting-edge research in science and technology.

Dr. Indraneel Mukhopadhyay is a Professor and Head of Institute at Amity Institute of Information Technology, Amity University Kolkata, with over 22 years of academic and administrative experience and 4 years of industry experience across India and the USA. He holds a Ph.D. in Computer Science & Engineering, an M.S. in IT from Clark University, and professional certifications from Harvard Business School Online, IBM, and CMI (UK). His research portfolio includes 5 books, 15 book chapters and 52 journal/conference publications, 10 granted patents, and 6 funded projects. He has led international workshops and faculty development programs on cybersecurity, digital technologies, and emerging computing across India, Singapore, Canada, and the USA.

Interdisciplinary Journal of Computing & AI

IJCAI
Interdisciplinary Journal of Computing & AI

IJCAI

RESEARCH

Artificial Intelligence in Rural Water Governance: Challenges, Opportunities, and Sustainable Pathways for India

Abhisikta Basu[1*], Avishikta Chatterjee[2], Debarghya Kundu[3]

[1,3]IEM's International Institute of Juridical Sciences (IIIJS), University of Engineering and Management, Kolkata;
Email - [1]abhisiktabasulaw@gmail.com, [3]debargha.kundu2003@gmail.com
[2]Department of law, Stockholm University, Sweden; Email - avishiktachatterjee.law@gmail.com

ARTICLE INFO.

Keywords: Water governance; Artificial intelligence, Rural India, Sustainable water management, Public policy
∗Corresponding author email address: abhisiktabasulaw@gmail.com
Manuscript received: 6 February 2026/Accepted April 16 2026
Published online: 17 April 2026
https://doi.org/10.5281/zenodo.19625242

Cite as: A. Basu, A. Chatterjee and D. Kundu, "Artificial Intelligence in Rural Water Governance: Challenges, Opportunities, and Sustainable Pathways for India", Interdisciplinary Journal of Computing & AI (IJCAI), vol. 1, no. 1. Aspiration Publishing Trust (DARPAN ID: WB/2025/0887371), p. 86-121, Apr. 2026. doi: 10.5281/zenodo.19625242.

ABSTRACT

Experts predict that by 2025 water demand will increase 55% leading to severe water scarcity. Artificial intelligence (AI) has the potential to revolutionize water management, and optimize water usage and improve efficiency in managing water resources, especially in developing nations like India where poverty and limited resources pose challenges. Despite its benefits, AI faces technical challenges, data security, ethical dilemmas, and stands out to be barriers for small-scale farmers. Addressing these issues and maximizing AI's potential can lead to significant improvements in global water security and agricultural sustainability, in rural India. TaKaDu, an Israeli water management system, powered by artificial intelligence, is gaining international recognition for its 24/7 monitoring platform that effectively tracks leaks and faulty taps, saving water, time, and money. In 2020, Tucson, Arizona implemented AI technology from VODA.ai to proactively manage its water system, predicting pipe breaks using machine learning. If we

simultaneously analyze these models the Israeli water conservation system can be implemented in the Indian scenario, with some changes. With the growing population and diminishing water resources, India faces challenges in water management, especially in rural areas where water scarcity poses threats to agriculture, health, energy, and the environment. In rural India, ineffective water monitoring not only exacerbates scarcity but also exposes communities to serious health risks arising from contaminated groundwater. By harnessing AI's capabilities for real-time monitoring, accurate predictions, and improved decision-making, India can enhance its water management practices and create a more sustainable future. This paper will focus on different schemes like Jal Shakti, Jal Sanchay, Jal Jeevan, PM Krishi Sanchay Yojana etc., for rural water management and highlight how implementation of AI presents significant opportunities to transform water management practices in India and globally, promoting sustainable agricultural practices, efficient water usage, and improved water security for all.

1 Introduction

India’s rural water governance structures appear to be at a crossroads, where the institutions, ecology, and legal systems are all failing in their efforts to manage the country's water resources. The traditional form of environmental law in India, which is still very reactive and enforcement-minded in nature, is often challenged by the impacts of climate change, groundwater depletion, poor water quality, and increasing demands in domestic and agricultural use. There is a lack of information on water governance and protection in India, despite the fact that the country has a vast body of laws on environmental protection and water resource management. In light of these structural challenges, the application of artificial intelligence (AI) and data-driven technology has been identified as a promising approach to water governance. AI-based systems, through real-time monitoring, predictive analysis, and decision-support systems, have the potential to improve regulatory capacity by transforming water governance from a reactive enforcement approach to an anticipatory and continuous regulation approach. In the context of rural water governance, these technologies have the potential to improve groundwater observation, identify contamination, predict water shortages, and optimize infrastructure planning. Nevertheless, the application of AI technology in environmental governance not only improves the efficiency of administration but also changes the very nature of regulation by transforming how regulatory knowledge is constructed, discretion is exercised, and accountability is allocated. This raises fundamental legal issues that need to be addressed. Existing concepts of environmental

regulation in India are based upon administrative discretion, post-facto enforcement, and judicial control. However, a system of regulation inspired by artificial intelligence is based upon probabilistic reasoning, prioritisation by algorithm, and automated forms of insight which may both inform or control human decision-making in this regard. While this may be to the advantage of such systems of regulation, it is also argued to undermine fundamental concepts of legality, transparency, decentralisation, and democratic accountability in the context of rural environments which exhibit socio-economic inequality and a lack of effective mechanisms for addressing grievances. Essentially, the question is not whether artificial intelligence is feasible in the context of rural water regulation, but to what extent its incorporation changes or influences fundamental concepts of regulation or legality.

In light of this, this study addresses two related research questions: first, how and to what extent would the incorporation of AI into India's rural water governance alter the traditional models of environmental regulation, and what legal protections would be required to maintain accountability and legitimacy in such a change? This explores how data-driven decision-support, predictive analytics, and ongoing monitoring alter regulatory power, discretion, and institutional accountability, this study situates AI within the larger framework of regulatory governance theory. The study conceptualizes AI as a type of regulatory modality whose use has moral and constitutional ramifications rather than as a neutral technological tool.

Secondly, in the comparative experience of AI-Enabled water governance three countries have attained significance: Israel, Singapore and the Netherlands. In this comparative study it is revealed that such countries have a spectrum of different social, political and economical approaches to AI regulation and water management. We identify a model of centralized sovereignty another model of public utility and a model of decentralization. The model of centralized sovereignty is revealed in Israel, reflects the statutory state ownership of all water resources consolidates planning, regulation, and AI-enabled monitoring within a single national legal authority [1]. Singapore demonstrates the statutory public utility model, where a single statutory regulator incorporates smart grid and AI-enabled monitoring technology into a legally codified public utility framework without changing the institutional power dynamics [2]. Whereas Netherlands reflects the coordinated decentralized approach with legally independent regional water boards integrating AI-assisted predictive management into a polycentric governance structure synchronized by national statutory frameworks [3]. In larger and more demographically complex states legislative fragmentation and federal transaction becomes impediment in regulatory design. As a result, these jurisdictions are analysed as unique points of reference for comprehending how AI might be incorporated into various legal frameworks rather than as transplantation models. Through such comparative experiences, the paper aims at deducing design principles instead of any institutional models for the Indian context. These design principles would

involve legal institutionalisation around data as a regulatory tool, the development of accountability for algorithm-assisted decision-making, checks to prevent any technocracy, and the maintenance of democratic participation in data governance scenarios. This comparative exercise will highlight aspects on the role of law in enabling, limiting, or sanctioning the regulation of AI governance for the environment.

The paper's methodology combines regulatory theory, comparative public law ideas, and doctrinal study of Indian water and environmental law in a techno-legal and regulatory governance approach. It makes the case that legal institutions' ability to incorporate AI into inclusive, transparent, and democratically accountable regulatory frameworks is more important for the long-term viability of AI integration in rural water governance in India than technology advancement alone. By doing this, the article hopes to further a legally grounded understanding of innovation in environmental governance and add to the growing discussions on AI as a regulatory tool. Figure 1 shows the schematic view of the paper. After the introduction, the second part deals with the conceptual and operational foundation of Artificial Intelligence and Water Governance. The third section deals with the Legal and Institutional Framework for the Rural water Governance in India. The fourth part deals with the Comparative Experience of AI Enabled Water Governance. The fifth part deals with the Opportunities for Integrating Artificial Intelligence within India's Rural Water Governance Framework. The sixth part deals with the Artificial Intelligence, Risk, and the Fragility of Legitimacy in Rural Water Governance. The seventh part deals with Sustainable and Legally Viable Pathways for AI-Driven Rural Water Governance in India followed by the policy recommendation in the conclusion.

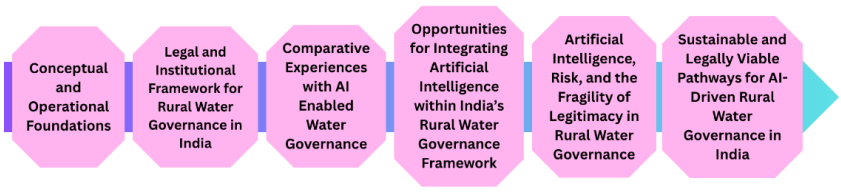


Fig. 1 A sequential framework outlining the conceptual basis, legal context, comparative insights, opportunities, risks, and sustainable pathways for integrating AI into rural water governance in India.

2 Artificial Intelligence and Water Governance: Conceptual and Operational Foundations

Artificial intelligence in the context of "water governance" refers to a group of computational technologies that include "machine learning," "predictive analytics," and "data modeling," all of which aid in processing vast amounts of "environmental" and "infrastructure-related" data [4]. It does not refer to the autonomously operating system with independent regulatory powers. Furthermore, when we discuss artificial intelligence in the context of "water resource management," we are referring to the integration of "remote sensors," "Internet of Things devices," and "predictive models" that aid in the "evaluation of groundwater levels," "quality," "scarcity," and "demand" [5], [6]. These technologies are more associated with "probabilistic predictions" than they are with "information systems."

It's important to note that AI technologies are not perceived as undermining human judgment, but rather as changing how knowledge relevant to regulation is produced. AI's impact on governance is reframed from responsive regulation to risk prediction, for instance, because of its potential for anticipatory or preventative regulation, particularly with regard to groundwater loss [5], [7]. The ultimate sovereign body still has the authority to enact laws, but algorithmic systems are increasingly dictating the agenda, risk, and resource allocation. This has resulted in a new type of algorithmic regulation that has important ramifications for accountability, transparency, and mandate.

2.1 Operational Architecture of AI in Water Resource Management

The operational application of artificial intelligence in water governance refers to the presence of an integrated software system that has an integration of data acquisition, analysis, and finally the outcome of regulations. At the fundamental layer, artificial intelligence and operational water governance employ technologies such as remote sensors, satellite image processing, and the Internet of Things to collect data on the following: groundwater levels, water quality parameters such as the presence of arsenic and fluoride contamination, rainfall patterns, and performance of infrastructures [5], [6]. At the analytical layer, the system employs artificial intelligence and operational water governance to process data and identify anomalies in the data collected at the previous layer, create probability-based predictions, and finally identify areas of regulatory stress or scarcity [4], [5].

Figure 2 conceptualises AI-enabled water governance by illustrating the connection between specific AI applications, the technological architecture that sustains them, and their associated governance outcomes. Key applications identified in the left column are leak detection, monitoring of groundwater quality, predictive analytics of scarcity, and optimisation of smart irrigation. The

middle layer represents the enabling infrastructure such as IoT sensors, remote sensing, machine learning algorithms, and decision support systems that convert environmental and infrastructural information into regulatory knowledge. The right-hand column indicates the corresponding governance outcomes, which include minimizing water loss, early detection of contamination, proactive planning, and enhanced agricultural sustainability. This model now illustrates how AI functions to become an integral component of a regulatory support system that reconfigures risk identification and resource allocation, despite the fact that the formal authority to make decisions is vested in the public institutions. This model is significant from a legal perspective because it enables the exercise of regulatory authority at multiple points in the system. Although the public institutions retain the formal authority to make decisions, the outputs of algorithms are increasingly shaping the evidence on which discretion is exercised. This creates a type of algorithmically mediated regulation that raises questions about accountability, transparency, and mandate [7].

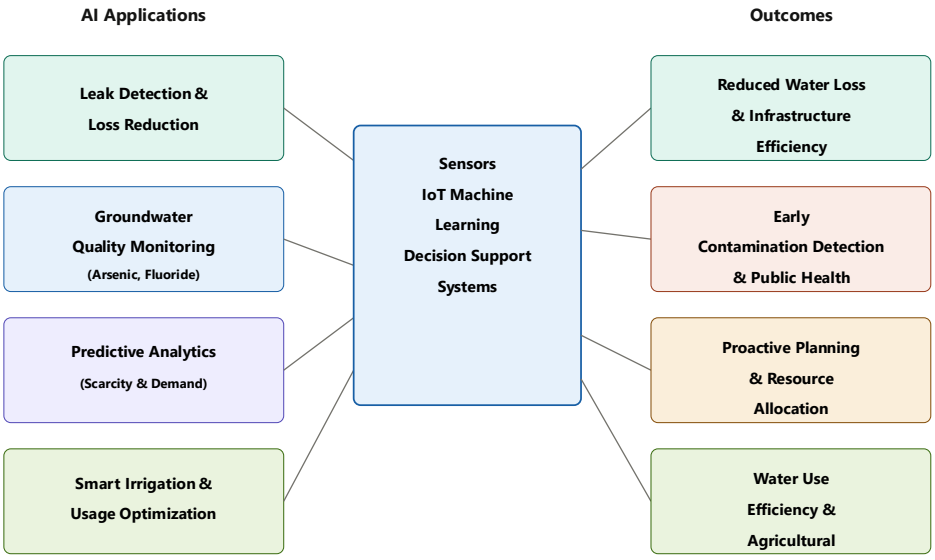


Fig. 2 Schematic representation of AI-enabled water governance showing the linkage between specific AI applications, the technological infrastructure supporting them, and resulting regulatory and governance outcomes in water resource management.

2.2 From Reactive Regulation to Algorithmically Mediated Governance

In Indian water governance, the previous conceptual frameworks for environmental laws have mostly been reactive, based on a model that promotes control and regulation only after a breach has been discovered. Conventional environmental laws are characterized by a compliance-enforcement system that often requires these regulatory mechanisms to respond to those who have violated environmental laws only after an infringement has been reported [8]. The introduction of artificial intelligence techniques, however, has given water governance a new sense of anticipation that goes beyond traditional reactive regulation strategies to one that is predictive to a level above a simple non-compliance condition [7]. However, this mode of anticipatory regulation has its own normative and institutional issues. In other words, the systems of prediction are based on probabilities instead of factual violations. Moreover, any decision made by the algorithmic model will impact the livelihoods, autonomy, and access to vital resources of individuals [9]. It has been argued that even though AI does not supplant traditional regulatory authority, it reconstructs how regulatory knowledge is constructed and how administrative discretion is exercised, and therefore, it acts as a modality of regulation an algorithmically mediated layer of regulation instead of an actual regulator [7].

This shift makes traditional accountability frameworks more difficult to understand since regulatory outcomes might be impacted by proprietary datasets, opaque models, or technical assumptions that are difficult to verify within current administrative law frameworks [9], [10]. In order to maintain transparency, mandate clarity, reviewability, and democratic legitimacy, the shift toward algorithmically mediated, anticipatory governance thus calls for careful institutional and legal calibration. Examining India's institutional and legislative structure for water governance is necessary within this context.

3 Legal and Institutional Framework for Rural Water Governance in India

The Indian government states that states should control all water resources which exist within their respective territories. The Indian Constitution establishes that states should have authority to create water-related legislation. The Seventh Schedule contains this information which functions as a state authority control list. The document identifies water supply needs for citizens together with farming irrigation support through canal construction and drainage management and water storage operations. States have the authority to manage their water power resources through their own decision-making processes. The law creates special rules which apply to rivers that cross state boundaries because the Indian Constitution establishes

regulations for these situations through Article 262 and Entry 56 of the Union List. Water stands as an agreement which allows states to determine all decisions about water resource management and storage facilities and power generation from water resources. The legal system divides water management responsibilities which show the country has a system for controlling water resources. The states maintain complete authority to create regulations which control water resources in their territories including agricultural and residential water distribution. The states have the authority to manage water resources which they can use for water distribution and irrigation systems [11]. The Union Parliament maintains legislative authority to establish rules about water which flows between different states through inter-state water systems. The Union Parliament creates laws which govern the use of state waters.

The Indian Constitution does not expressly provide a standalone fundamental right to water. However, the judiciary has consistently interpreted Article 21 of the Constitution which guarantees right to life and personal liberty encompassing various unenumerated dimensions of life and livelihood. The right to live with human dignity has been incorporated into Article 21 through broad judicial interpretation, and access to adequate and safe water has been acknowledged as an essential component of the right to life. The jurisprudential foundation for this position was clearly articulated in *Subhash Kumar* v. *State of Bihar* [12], where the Supreme Court held that the right to life includes the right to enjoy pollution-free water and air for the full enjoyment of life. The Court explicitly stated that environmental degradation affecting water quality violates Article 21 [13]. Subsequent judgments have reaffirmed this position. The Court in *A.P. Pollution Control Board* v. *Prof. M.V. Nayudu* [14] emphasized the significance of having access to clean drinking water and acknowledged that water is a basic necessity for living and requires strict regulatory supervision. Similarly, the Court noted that water is a fundamental human need and an important part of the right to life under Article 21 in *Narmada Bachao Andolan* v. *Union of India*, [15] in deciding cases involving dam development. Moreover, the Supreme Court highlighted the preservation of water resources and the environment as public trusts in *Hinch Lal Tiwari* v. *Kamala Devi* [16], connecting these duties to Article 21 of the Constitution. As a result, even though the Constitution does not specifically list a "right to water," court interpretation has solidly incorporated water rights especially the right to clean and drinkable water within the broad purview of Article 21.

3.1 Legal Framework relating to Water Management in India

The legal framework for water resource management in India consists of various laws. The Water Act serves as the primary legislation which handles water quality standards throughout various regions. The Water Act functions as the Water (Prevention and Control of Pollution) Act, 1974 [17] to establish water

quality standards for all regions. The Water Act serves as a law which protects India from water contamination while it protects all water bodies that exist in the country. The Water Act functions as a vital tool which enables India to manage its water resources through its system of water resource management [18]. The Water Act functions as a part of the legal structure which regulates water resources throughout India. The Act established the Central Pollution Control Board under Section 3 and State Pollution Control Boards under Section 4 as organizations which maintain water cleanliness. According to Section 17 of the Act the State Pollution Control Boards operate independently to perform water pollution assessments and they need to show their authority for water quality testing and document evaluation and rule enforcement. The central government makes sure everyone follows the rules all over the country. The law establishes particular rules which govern all water bodies that exist in rural areas which get contaminated through sewage and agricultural waste.

The Central Pollution Control Board together with State Pollution Control Boards serve as essential organizations which protect our water bodies from pollution.

The Environment Protection Act operates under the name EPA as a legal framework which defends our natural surroundings. The Water Act functions alongside this law which they both operate together. The Indian Constitution created the EPA through its Article 253 which serves as its legal foundation. The article requires nations to implement all international agreements which they have previously signed. The EPA grants the government extensive authority to protect both our natural environment and our water resources. The Environment Protection Act functions as the EPA which enables the government to perform necessary actions for protecting our environment and water resources [19]. The government holds authority to perform environmental protection activities which safeguard all natural resources including water bodies that exist throughout national territories. The government needs to protect environmental resources together with water supplies because they hold major importance. The government holds responsibility to protect environmental health in all regions which include both rural and metropolitan areas including major cities. The protection of water resources stands as a fundamental requirement for this mission. governing body.

The ‘Central Ground Water Authority serves as a fundamental resource which enables water resource management. Groundwater requires the most urgent attention when it comes to water resource management. The Environment Protection Act created the Central Ground Water Authority as its established governing body The ‘Central Ground Water Authority’ has the responsibility to protect all groundwater resources which are used by people for their needs. The country needs to handle its groundwater resources through both protection systems and management systems. The agreement serves as a solution which helps people who reside in rural areas. The community depends on groundwater resources. The community operates numerous borewells. The ‘Central Ground

Water Authority' issues 'No Objection Certificates' to people who require groundwater access for their purposes. The document provides instructions which guide people to protect their water resources while ensuring environmental safety and groundwater replenishment. The Central Ground Water Authority works to protect our groundwater supply which exists in sufficient quantities [20]. The Central Ground Water Authority functions under the Environmental Protection Agency to handle problems which exist outside the scope of current legislation. The national government lacks any established laws which protect groundwater resources. The Central Ground Water Authority is working to solve the existing groundwater problem.

The Supreme Court of India delivered a vital ruling during 1999 which involved the A.P. Pollution Control Board against M.V. Nayudu case. The Supreme Court of India established that the state must establish proper systems to defend its water resources from any harm. The state must follow environmental and water laws because these regulations require them to do so. The Supreme Court of India requires states to develop systems which will defend their water resources. The Supreme Court of India views this matter as an essential component which belongs to environmental protection work. The *A.P. Pollution Control Board,* v. *M.V. Nayudu* case [14] shows that the state has a responsibility to protect the water resources as part of environmental laws [21].

3.2 Policy and Administrative Schemes

The government has established rules which operate through systems to provide clean water access for residents who live in various regions. The established rules receive support from national plans and programs which ensure rural communities access safe drinking water. The Government of India established the Jal Jeevan Mission (JJM) as their official program. The JJM aims to deliver drinking water through dedicated taps to every rural home before the year 2024. The JJM operates through a core system which protects water sources and performs water testing and educates communities about water purity and encourages local participation in the Jal Jeevan Mission. The JJM maintains its status as an essential program which provides water resources to rural populations. The Ministry of Jal Shakti has established particular directives which Jal Jeevan Mission leaders must follow to perform their duties. The group wants to make sure the Jal Jeevan Mission works through their preferred execution method [22]. The Ministry of Jal Shakti monitors the Jal Jeevan Mission to ensure all activities follow the established operational guidelines.

The Jal Shakti Abhiyan (JSA) operates as a water conservation initiative which works to protect every drop of water while establishing systems for sustainable water resource management. The Jal Shakti Abhiyan focuses on two main objectives which involve rainwater storage and groundwater reservoir expansion and environmental protection for water-related ecosystems. These things are very important for getting water to people who live in villages. The Jal Shakti Abhiyan operates its water supply activities because certain regions lack access to water resources. Although the JSA provides an institutional mechanism for

rural drinking water services and source sustainability, its operational guidelines do not include a mechanism for artificial intelligence-based monitoring and predictive decision support systems. This paper argues that AI-based tools can be normatively and institutionally integrated with the existing Jal Jeevan Mission to enhance source sustainability, groundwater protection, and climate resilience. The integration will not alter the legal authority of the Mission but will improve its evidentiary and anticipatory capabilities within the existing administrative structure.

Figure 3 is a conceptual model showing the potential institutional integration of AI tools into initiatives for rural water conservation and climate resilience. The left side column mentions the AI applications for rainfall and runoff modeling, geospatial AI and computer vision, groundwater recharge and quality assessment, and decision support systems for watersheds. The right-side column mentions the ecological and governance outcomes of the AI applications, which include efficient rainwater harvesting, conservation of traditional water bodies, groundwater recharge, and climate-resilient watershed development. The arrows represent the process of translating environmental data into decision-support systems. This model takes into account the AI application as a decision support system in the existing governance framework but not as a regulatory authority.

Fig. 3 Proposed Integration of AI Tools within Rural Water Conservation Frameworks

The Pradhan Mantri Krishi Sinchayee Yojana is another thing. The Pradhan Mantri Krishi Sinchayee Yojana wants to make use of water for irrigation. The Pradhan Mantri Krishi Sinchayee Yojana aims to provide water access to every agricultural field through its program which they call "Har Khet Ko Paani". The Pradhan Mantri Krishi Sinchayee Yojana includes water preservation methods which help farmers produce higher crop yields [23].

The government uses these systems as operational guides which help them manage their official responsibilities. The government follows these guidelines to direct its operations because these documents do not possess legal authority. The organization members possess strong influence because they channel financial support to appropriate locations which enables them to establish customized state strategies and perform monitoring activities. The courts have declared these schemes essential for State performance because they enable people to access safe drinking water and clean water which the State needs to provide under Article 21.

The main objective of 'JJM and JSA missions' moves beyond simple legal compliance. The leaders of these operations establish conditions which states must follow to obtain funding along with other forms of support. Things operate by following this system. The government must act because Article 21 establishes that people require basic water availability. The government needs to follow JJM and JSA because these documents guide their operational strategies although they do not possess legal authority.

3.3 Institutional Architecture and Governance Challenges

The rural water sector in India receives assistance through a hierarchical system which operates through different levels. The system connects three levels of government which include the national government and the state government and the local government. At the level there are ministries such as the Ministry of Jal Shakti. The Ministry of Jal Shakti creates water sector policies for India which the government funds while monitoring their operational success. The Ministry of Jal Shakti maintains partnerships with water-focused organizations which include the CPCB and the CGWA and the water mission directorates. The water sector in India receives support through the combined efforts of these organizations.

The state level requires water authorities including water boards and irrigation departments to enforce all established regulatory requirements. The organization develops strategies which match the actual state of water resources. The states maintain their right to develop water regulations through their established authority. These laws serve to fulfil state-specific requirements through their establishment of guidelines for groundwater management and canal operations. The organization establishes rules which determine how water should reach the population that requires it. The state pollution control boards actively participate in this procedure. They help keep the water clean.

States have the authority to create water-related regulations which only affect their specific jurisdiction. The Panchayati Raj Institutions serve as vital resources for water resource management throughout their operational areas. They must handle all operational aspects which require their attention. The Gram Panchayats maintain responsibility for developing and operating water supply systems which they control. The state government has granted these organizations the power to carry out this work. Article 243G of the Constitution enables Panchayati Raj Institutions to provide essential services which include drinking water and sanitation and hygiene facilities for their communities [24]. The Panchayati Raj Institutions function as active participants in each of these activities. The organization needs to solve its current work challenges while it needs to confirm that all employees follow company rules. The federal government and the states have some overlap, which can cause problems with our water policy. The situation leads to state water disputes which fail to reach proper solutions.

We need to apply the rules from Article 262 to work through the solutions for these existing problems. The people who handle water management in towns and villages face two major challenges because they lack both proper training and sufficient financial resources to perform their duties effectively. The current water management systems we operate will probably fail to produce good results when used in the future. The water schemes lack sustainability because the community members who should manage them do not have enough knowledge or money or technical skills to run them correctly. Water schemes create problems because of the following situation. The three institutions which control pollution and provide water and run local government systems fail to work together effectively which leads to weak control of rural water quality and pollution levels that affect community health.

3.4 AI in Rural Water Conservation and Climate Resilience

There is growing recognition that AI is a crucial enabling tool for water conservation measures in rural areas. Areas that are facing problems with groundwater depletion, rainfall fluctuation, and hydrologic variability as a result of climate change require water conservation measures [25]. The authorities' tardiness and the lack of coordinated efforts have been cited as reasons for criticizing the current water conservation strategies [26]. Improved predictive analysis and risk assessment in the future are guaranteed by AI systems. Figure 2 shows how AI tools used in rural water conservation are functionally linked to the corresponding governance and ecological outcomes. The key AI-based tools mentioned in the left column are rainfall-runoff modeling, computer vision and geospatial analysis, groundwater recharge and quality analysis, and predictive decision support systems. Although the right column highlights outcomes such as successful rainwater harvesting, sustainable groundwater recharge, revivals of traditional water bodies, and climate-resilient watershed planning, the central arrows indicate the conversion of environmental data into valuable insights.

Substantively, these technologies provide scope for the early identification of stress areas, variability of recharge, and seasonality of scarcity through the use of machine learning and architecture of remote sensing platforms [25], [26]. These layers are interdependent parts of a system, not a linear sequence of a process, wherein hydrological modeling feeds the analytics of recharge, and the consequences of conservation strengthen long-term resilience in the watershed basin. Though AI systems enhance decentralised systems and institutions, like the Gram Panchayat, through stronger evidence base of decision-making, they pose normative questions of probability in governance, data asymmetry, and accountability [19]. AI-based rural water conservation must therefore be seen not only as the modernization of water conservation but, more substantially, as a shift towards a preventative system of environmental governance.

4 Comparative Experiences with AI Enabled Water Governance: Legal and Regulatory Models

The experiences of Israel, Singapore, and the Netherlands reveals a spectrum of different approaches to AI regulation and integration in water management: a model of centralised sovereignty, a model of statutory public utility, and a model of coordinated decentralisation, respectively. The model of centralised sovereignty is represented by the experience of Israel, where state ownership and control in accordance with the Basic Water Law facilitate a single entity's control over water data and real-time compliance assessment in a vertically integrated system. The model of statutory public utility is represented by the experience of Singapore, where AI is part of the PUB's regulatory model to improve water efficiency and accountability without affecting the allocation of power between institutions. The model of coordinated decentralisation is represented by the experience of the Netherlands, where AI technologies are used by autonomous regional water boards to improve predictive management in a harmonised but polycentric system of water management based on institutional coordination and data interoperability.

4.1 Israel: Centralized Legal Mandate and AI-driven Water Monitoring

The Israeli national law on the legal cut-off can be traced to the Basic Water Law in 1955 [1], which was based on the principle of all the water resources, located within the territory of the State of Israel, to belong to the State as properties, and that possessing of water resources as property does not exist. The law entrusts the executive of all powers of decision making and appropriate use of water resources to the national level by depriving the sub-national authorities of the options of autonomous management of water resources. The other feature of the Israeli water regulation system is the national legal authority on ownership and administration of the water resources [27].

In the given framework, planning, regulation and management of the overall water sector, including ground water, drinking water supply, desalting output, waste water reuse, interregional transfer system of water like the National Water Carrier lies in the hands of the State of Israel through national crisis management agencies.

This government ownership has facilitated the joint effort in water usage, conservation, drought resistance, and water real-time observation. Israeli legal system reflects such policy orientation of the legislative and administrative level which prioritizes collective sustainability and equitable distribution, which are impermissibly connected with compliance and enforcement regime within the territory.

The Israeli Water Authority is the top of the national water management system in Israel, as it is a government structure and it is positioned under the Ministry of infrastructure and water issues [28]. Planning, regulatory, quality and supply in the water sector in Israel has been devolved to the Israeli Water Authority which serves as a centre of policy making and management in the sector [28]. The duties of the Water Authority may entail the following: Ensuring the long-term availability of water: quality, amount, and financial consistency Event managing sewage and effluent water to the desired levels; Coordination of national policy through the Water Authority Council- multi ministerial organ that permits prominent strategic choices. The governance model puts the heavy regulatory burden on the national level with the orientation being on efficiency and national compliance. This model also supports the international and regional transboundary water cooperation of Israel, by incorporating the data and monitoring needs in the broader legal systems.

Within the past few years, the state of Israel has been using artificial intelligence technology within its water governance and compliance system. Although the primary legislation has not yet incorporated AI on a statutory level, the application of the same is already being carried out on an operational level by state actors such as Mekorot, which is the national water carrier in Israel. For example, Mekorot has installed AI-capable monitoring systems such as the "AquaRing" system in remote stations of the National Water Carrier system [29]. It uses machine learning and spectral analysis to provide timely alerts for water quality, safety, and other unexpected trends, and has minimized response times for detection to ensure that these comply with national water quality standards. The AI-powered data analytics platforms are increasingly incorporating data from remote sensors that can enable the authorities to make anticipatory decisions and point out potential problems with respect to contamination, pressure anomalies, and inefficiencies in the system [30]. The platforms are synthesizing millions of data points every day in their support of compliance verification and responsiveness in the water governance system. Consequently, this implies that the integration of AI tools is effective in extending the Israeli legal regime's ability to monitor continuous compliance, thus aligning

technological development with the legal requirements at the national level that regulate water as a public good.

4.2 Singapore: AI within statutory public utility regulation

The Singapore water regulatory framework is a statutory framework that is codified under the Public Utilities Act and enforced by the Public Utilities Board (PUB), which is the National Water Agency in Singapore. The Public Utilities Act (Chapter 261) [2] is the statutory framework under which the water sector in Singapore is regulated; it provides for the establishment of the PUB as the sole statutory authority that regulates the water supply sector [2]. As provided for in the Act, one of the PUB's functions is to ensure that water resources are provided sustainably and efficiently at all stages, from catchment and production to distribution, treatment, and reclamation [2]. The regulatory function of PUB encompasses water quality, supply reliability, pricing, and infrastructure robustness [30]. The legislative approach adopted by the Singaporean government recognizes the fact that water is a public utility that requires comprehensive regulation throughout the value chain. In this regard, PUB is the main actor that has the ability to license, regulate technology standards, control operations, and enforce compliance with the statutory requirements set out under the water safety regulations, including the Environmental Public Health (Water Suitable for Drinking) Regulations [30].

The Smart Water Grid project in Singapore is the institutional manifestation of the need to integrate digital and AI technology into the legal framework of water governance [31]. PUB has systematically developed sensoring, digital communication, and analytics infrastructure in the water distribution sector to facilitate real-time monitoring and decision support.

These smart technologies enable automatic leak detection, anomaly detection, and predictive maintenance that will improve PUB's regulatory control by minimizing non-revenue water, optimizing asset management, and facilitating proactive measures to address system breakdowns before they cause supply continuity problems [31].

Smart water meters, together with AI-informed analytics, not only provide optimization for PUB's operational efficiency but also strengthen the framework of compliance reporting in accordance with the Public Utilities Act [32]. The smart water meters provide daily automated consumption reports through a digital network in a secure manner, thus improving transparency and regulatory compliance by synchronizing consumption behavior with regulatory efficiency standards [32]. In Singapore, AI and digital monitoring technologies have, therefore, become essential components of regulatory accountability to support PUB's supervisory role in accordance with the requirements of national utilities law.

4.3 Netherlands: Predictive Water Governance and Institutional Coordination

These intelligent technologies provide for automatic leak detection, anomaly detection, and predictive maintenance that will enhance PUB's regulatory control function by reducing non-revenue water, ensuring effective asset management, and enabling proactive responses to system failures before they result in supply shortages [31]. The smart water meters, together with AI-related analytics, not only play a crucial role in ensuring the optimal efficiency of PUB but also facilitate the enforcement of the compliance reporting framework as stipulated in the Public Utilities Act [32]. The smart water meters have the ability to automatically transmit their readings on a daily basis via a digital network in a secure manner, hence enhancing the transparency and enforceability of regulations by ensuring that consumption behavior is consistent with the regulatory efficiency standards [32]. AI and digital monitoring technologies have, therefore, become a critical component of regulatory accountability in support of PUB's supervisory role in Singapore.

The Netherlands has a multi-layered system of water governance, which is based on constitutional obligation, statute, and decentralized powers, and which seeks to balance national policy guidelines, regional autonomy, and decentralized responsibilities [33]. The Dutch system of water governance is famous for its high degree of institutional coordination and development towards integrated flood and water resource management [33]. Unlike the highly centralized systems of, for example, Israel, for example, the Dutch system is characterized by decentralization and functional coordination between the national government, the provinces, and the regional water authorities (water boards), which are specialized public bodies entrusted with the statutory authority to manage water systems. These regional water authorities are legal entities distinct from the state and have the legal duty to exercise continuous control over surface water, flood defenses, drainage, and water quality in specific hydrological areas [34]. The regional water authorities have the powers to make bylaws, license, tax, and perform all acts and operations as provided for in the Regional Water Authorities Act [34].

The framework of institutional coordination in the Netherlands is based on collaborative governance structures such as the Delta Programme, which involves national government departments, provinces, municipalities, water boards, and other stakeholders to develop overall resilience strategies for climate change, sea-level rise, flood risk, and sustainable use of water resources [35].

The governance ecosystem now recognizes AI systems together with digital technologies as helpful tools for predictive water management through their ability to track groundwater levels and their ability to forecast floods and generate early warning alerts. The Netherlands needs to establish specific laws about AI usage for water management but regional authorities together with

Rijkswaterstaat have started developing systems which combine past hydrological information with current sensor data to enhance their prediction capabilities for dealing with climate changes [36]. Authorities must share data according to the principles of predictive governance because water boards together with national authorities exchange standardized environmental information and they conduct system modeling with risk evaluation and operational scheduling. The flow of data between institutions serves as input for regulatory bodies to develop proactive public safety protection measures which prioritize water system resilience. The Netherlands needs predictive water governance to function because it depends on institutional coordination through robust statutory rules which modern water management institutions operate with AI systems and data sharing technology [37].

5 Opportunities for Integrating Artificial Intelligence within India's Rural Water Governance Framework

The comparative experiences highlighted in the previous section show that there is a common understanding that informs the regulation of water governance through the use of artificial intelligence: that is, the transformative potential of artificial intelligence in water governance is realized not when the latter is treated as a technological intervention but when it is treated as a mode of regulation in law. This is especially pertinent in the context of India, which has a tradition of rural water governance that is heavily influenced by a broad but not very effectively operationalized legal regime. The Water (Prevention and Control of Pollution) Act, 1974 [38], and the Environment (Protection) Act, 1986 [39] are examples of legislation that grant broad powers in the regulation of water but whose actual effect in rural water governance is limited due to information problems and the delay in the implementation of the law [40].

From the regulatory governance theory perspective, the challenge with rural water systems is not the lack of norms but the inability of the regulatory institutions to continuously observe, interpret, and react to the intricate environmental situations. The traditional command-and-control regulatory model is based on the presumption of known facts and known violations, which is questionable in the context of the uncertain, non-linear, and cumulative effects of climate change on rural water systems. AI, with its capacity to aggregate large volumes of data, can help achieve what regulatory theorists term information-centered regulation [41].

5.1 Real Time Water Quality and Quantity Monitoring as Continuous Regulation

Monitoring has always been in a marginal position in Indian water regulation. Although environmental legislation has formally acknowledged the importance of monitoring in the context of enforcing water regulations, the lack of manpower, financial, and geographical resources has constrained the role of

monitoring in Indian water regulation, particularly in rural areas. The absence of documentation of groundwater extraction, rural water quality, and infrastructure efficiency has led to reactive and sometimes incomplete decisions by Indian water regulators [42].

The development of AI-based sensor technologies and machine learning technologies promises to revolutionize the role of monitoring in Indian water regulation by enabling the continuous and real-time monitoring of rural environments [43]. From a regulatory theory perspective, the development of AI-based technologies and machine learning technologies promises to revolutionize Indian water regulation by enabling the transition to continuous regulation, whereby compliance is viewed as a continuous process rather than an event.

The regulatory importance of this change is considerable. Monitoring minimizes informational asymmetry between the regulator and the regulated, a perennial problem in rural environmental regulation. It also increases the legitimacy of legal standards by making the enforcement of the law less arbitrary and more informed [44]. What is particularly noteworthy is that these advantages do not require any expansion of the regulator's powers. Instead, AI increases the effectiveness of the enforcement of existing legal standards by providing the necessary information for their exercise.

Nonetheless, as the literature on regulatory theory points out, monitoring is not a neutral activity. What is monitored, how the data is interpreted, and who has access to the data are normative decisions. What the advent of AI offers is not the generation of data per se, but the integration of the monitoring system into the legal standards and requirements for monitoring [45].

5.2 Predictive Analytics and the Restoration of Water Regulation Towards Prevention

Traditionally, Indian rural water governance has followed a reactive regulatory paradigm. In this model, regulatory and legal interventions are made in response to water contamination, depletion, or system failure. This reactive approach to water governance mirrors the more general command and control approach to environmental governance. This approach assumes stable environmental conditions and violations. Such assumptions are no longer tenable in the face of climate change, where water risks are gradual, contextual, and often cross-boundary.

The advent of predictive analytics using AI offers the potential to break out of the reactive regulatory paradigm and develop anticipatory and preventive approaches to water governance. This is because, through the use of historical data coupled with climatic, land, and consumption patterns, AI predictive analytics can help identify potential risks before they escalate into violations or

crises. This, therefore, creates an opportunity to develop a water governance system that is anticipatory in nature [46].

The development of such a process holds wider normative implications for environmental law in India, which judicially has acknowledged the precautionary principle but has never operationalized it as an administrative practice [47]. Predictive analytics holds the prospect of providing a tool for the operationalization of the precautionary principle as an administrative practice for the very first time, thereby empowering the state to take early interventionist measures. The danger here comes from an aspect of regulatory theory that warns about the potential for predictive analytics to obscure uncertainty and perpetuate biases. The opportune thing to do here is to utilize predictive analytics as a tool for judicial reasoning and judgment [48].

5.3 Evidence Based Planning, Resources, Allocation, and Adaptive Governance

Another opportunity provided by AI comes in the area where there can be bridging of the space between policy formulation and hydrological conditions at a local level for rural water governance. For instance, large-scale initiatives such as the Jal Jeevan Mission and the PM Krishi Sinchayee Yojana have been concerned with developing infrastructure and coverage targets, where certain assumptions are made during the formulation. While this has assisted in improving access to water, it has also led to concerns about sustainability, source reliability, and equity [49].

From the perspective of water governance, AI can assist in integrating various data sets related to water availability, agricultural demand, demographic changes, and climate change. This is useful in moving towards adaptive regulation, where regulatory strategies change over time in response to new evidence, as opposed to static approaches that assume regulatory strategies will remain the same. The significance of adaptive governance is now widely recognized in environmental law [50].

In decentralised systems, particularly Panchayati Raj systems, access to such analytical capabilities may assist in the participation of the system in the regulatory systems. Despite being constitutionally empowered, decentralised systems are often not informational resource-rich enough to engage with other systems [51]. Being constitutionally empowered as shared informational systems, AI systems may assist in the resolution of the capability issue for decentralised decision-making systems without undermining decentralised decision-making. This is reminiscent of the theory of polycentric governance, which is based on shared rules and information.

5.4 Transparency, Accountability, and the Democratic Potential of Data- Driven Regulation.

In India, transparency has been cited as one area that requires improvement in water governance in relation to groundwater extraction, allocation, and infrastructure management. This is an area where AI-driven water governance tools can potentially address the gap by enhancing the accessibility and understandability of regulatory information to various stakeholders.

Data visualization tools and reporting can potentially interpret and convey regulatory information in a manner that can be understood and utilized by various stakeholders in water resources management, such as the community and civil society organizations. In relation to regulatory governance in particular, there is a possibility that AI-driven mechanisms in water resources management can help in the improvement of responsive regulation. Responsive regulation refers to a regulatory activity aimed at using feedback provided by different stakeholders in the decision-making processes by regulatory bodies. According to literature, there exists no automatic connection between digitization and transparency in the management of water resources in India; as such, there is a need to enact laws that have touched on issues such as transparency in line with the use of technology in promoting democratic participation rather than technocracy.

The opportunity, therefore, would be the legalization of AI-driven transparency with community-centric approaches that treat the community as stakeholders in regulation rather than data subjects; this could potentially build up accountability and legitimacy in rural water governance models [52].

5.5 Opportunity as Regulatory Transformation Rather Than Technological Fix

Taking the issue into consideration, it can be fairly fathomed that the role of AI in assisting with water in country areas is not merely about efficiency or an upgrade to an old system. As long as we think of AI as a tool for making services more efficient, we will, to a great extent, miss the real regulatory meat that comes with AI [53] Technologically and legally, AI can actually change the way water law works; it will help us move from mere rules enforcement when something comes up to a more ongoing, information-driven approach to regulating things.

From the water governance point of view, AI systems can help to integrate different data sets on water availability, agricultural demand, demographic changes, and climate change. Looking at everything that has been written about how this regulation actually works, it's not really about putting down some rules for people to follow. It's really more of a constant thing, just watching and waiting, and trying to figure everything out. In India, as far as dealing with the regulation of water supply in the countryside, there is usually a huge disconnect between what the rules aim to do and what they actually are doing. It really

illustrates the level to which our systems can't keep things running the way they are supposed to. AI really excels when our old methods are no longer working quite as well as they used to. So, what does this really bring to the table? The opportunity to totally transform the way that regulatory body's function. This is not a superficial level; this is a really deep level. This is not really about looking backwards to determine whether or not the rules were followed. It's really about looking ahead to determine potential risk [54].

Significantly, what this is stating is not that the rule of law is superseded by algorithms. Rather, AI is underlining the need for legality to the extent that it makes the normative decisions that underpin the rule of law explicit. Determining what risks to act on, how those risks need to be defined, and what agency is to act in a regulatory manner all need to be spelled out in the law, not the algorithms [55]. Otherwise, it becomes a matter of a technocratic system beyond democratic or legal control. The opportunity, therefore, is not in the automation of such choices but in the legal-technological co-production of the definition of such objectives, limitations, and accountability.

These developments acquire a new meaning and significance if such a reframing is applied, and its connection with the topic is understood, especially when applying such a reframing to the Indian scenario, where measures undertaken under various governmental policies have, to a certain extent, eliminated the necessity for such measures to have a backing of any such legally constituted necessity. Moreover, this reframing of AI, as a regulatory tool, underscores the limits of governmental missions for the effective execution of digital measures and emphasizes the necessity for such measures to have a ground in the laws of the country [56].

Moreover, the regulatory perspective on AI brings out aspects related to the question of power, participation, and exclusion. Based on the theory of regulatory governance, the focus is on the potential of regulatory techniques to influence the power balance of institutions and stakeholders. In this regard, there is the potential for AI systems in rural water governance to marginalize local knowledge, which could be addressed through participation. This opportunity is thus also one that is committed to the values of participation, inclusion, and transparency.

It is thus evident that, in this regard, the AI solution is not one that solves the rural water crisis but one that offers an opportunity for the law to rethink the practice of environmental regulation in the face of ecological uncertainty and administrative constraint. The opportunity does not lie in the technology itself but in the extent to which the law enables, limits, and legitimates the AI system [56]. This connects to the next section, which will discuss the regulatory challenges of AI systems in rural water governance in the absence of legal safeguards.

6 Artificial Intelligence, Risk, and the Fragility of Legitimacy in Rural Water Governance

The one that keeps getting mentioned is how it would really help with water management in the countryside. I think they mean it would all just work better, give us more information, help us make decisions faster, and maybe even predict things better than we could on our own. However, the literature on regulatory governance has repeatedly argued that optimisation without legitimacy is unstable. When artificial intelligence systems are introduced into areas as politically contentious and socially embedded as water governance, they do not simply improve the capacity of governance; instead, they transform how power is exercised, legitimated, and contested. This section contends that the central challenge of AI in rural water governance is not failure but regulatory instability, the potential for governance systems to become less accountable, less inclusive, and ultimately less legitimate [57]. Instead of considering data, liability, ethics, and exclusion as separate issues, this section considers them as a set of interconnected points of instability in a single techno-legal system. Failure to address one tends to exacerbate the others.

6.1 Data as Infrastructure: From Informational Gaps to Informational Power

AI-governance is based on the premise that data poverty is a challenge that needs to be addressed. In rural water governance, however, data poverty is not an accident but a symptom of institutional neglect and an uneven state presence. It has been observed in recent policy studies that data on groundwater and drinking water in rural India is frequently patchy, outdated, or simply non-existent in the marginalized areas. If AI systems are trained on such uneven data geographies, they are likely to render historical invisibility as algorithmic irrelevance [58].

More problematically, there has been a shift from data as evidence to data as infrastructure, a resource that shapes future regulatory possibilities. Once the AI systems have made a determination of what is relevant data, the regions that do not have a digital footprint are likely to be out of the regulatory scope entirely. This has been noted in recent blogs on environmental governance, which have noted that “data poor regions are governance poor regions in algorithmic systems” [59].

The issue of ownership further cements this inequality. Many of the AI systems that are publicly available are developed by private companies, and as such, they retain control over the architecture of the data and the analysis that is being conducted. Without sufficient legal regulation over the issue of public ownership and access, the water data in rural regions could be locked away in private systems [60]. This is part of a larger concern that the digital public infrastructure is, in the absence of sufficient regulation, quietly shifting the balance of regulation from the state to the technology companies.

6.2 From Measurement to Surveillance Ethical Creep in Environmental Monitoring

The water governance system that relies on AI is contingent on the continuous measurement of water quality, usage patterns, groundwater levels, and infrastructure performance. At first, the concept of continuous measurement appears to be normatively unproblematic, if not welcome, in the wake of the scale of rural water problems [61]. However, recent developments in the literature and discourse on water governance have warned that continuous measurement could potentially creep into continuous surveillance, particularly in a context where there is a lack of legal protection and power imbalances.

This is what has been termed, in recent governance blogs, the phenomenon of ethical creep. This refers to the gradual extension of data beyond its original use in regulation. In the context of rural water governance, an AI system intended for the purpose of contamination or leakage detection may begin to profile household water consumption, agricultural patterns, or seasonal livelihood patterns [61].

Most importantly, environmental governance has continued to remain on the fringes of data protection debates. While Indian constitutional jurisprudence has recognized informational privacy as an integral part of the right to privacy, the extension of data protection with respect to sectoral governance has remained at an embryonic stage [62].

Furthermore, it has recently been contended that data protection literature has ignored the fact that data on the environment has been considered public data, thus overlooking the fact that it has the ability to reveal intimate socio-economic patterns when algorithms are employed on it [63]. The failure of data protection principles with respect to the use of AI monitoring on the environment has resulted in a vacuum that allows intrusive practices to flourish.

From a regulatory governance perspective, excessive surveillance may undermine the very purpose it sets out to achieve. The literature on legitimacy in regulatory governance suggests that communities are likely to be compliant with environmental regulations when they perceive such governance to be legitimate. In such scenarios, the use of AI-based monitoring systems, acting as opaque surveillance technologies, might negate such perceptions, as such histories may have existed, for example, in rural India. Ethical considerations, thereby, are not just desirable; they are functional imperatives [64].

6.3 Algorithmic Advice, Administrative Discretion, and the Dilution of Responsibility

As these AI systems transform their role beyond those of simple monitoring tools and towards their role as tools in decision-making, they inevitably have a part to play in the shaping of regulatory decisions. This may potentially include a role

in predictive analytics in decisions concerning infrastructure, drought, groundwater extractions, or emergency water supplies, among others. Though not ultimately responsible for actually deciding outcomes, recent research has noted that, in fact, these systems exert a powerful normative influence that ultimately limits the possible discretion in decision-making that administrative authorities possess.

This creates complex issues of accountability. Administrative law in India is based on principles of decision-making that are reasonable, transparent, and reviewable. However, these systems increasingly rely on probabilistic models that are not transparent, even to their creators. Recent blogs on law and technology have noted that this represents the emergence of "decision-making without reasons," where decisions are justified on the basis of technical authority rather than legal authority [65].

The result is a diffusion of responsibility. If the negative consequences of algorithmic recommendations such as the denial of access to water for some villages or the preferential treatment of some villages over others need to be explained, it is no longer clear who would be held legally accountable. This issue of diffusion of responsibility was addressed in recent literature on regulation as the phenomenon of structured deniability, where the absence of responsibility is systematically created rather than simply being possible.

In the context of rural water management, where grievance redress mechanisms are weak to begin with, the diffusion of responsibility is a particularly problematic issue. Without any legal obligation to explain and contest algorithmic recommendations, the risk of the gradual undermining of the ideal of the rule of law arises [66].

6.4 Procurement, Platforms, and the Quiet Reallocation of Regulatory Power

The governance implications of AI are typically considered at the level of outcomes, but recent policy debates have highlighted the importance of procurement as an area of regulatory transformation. Procurement decisions about which AI systems to use, on what terms, and with what standards are an important influence on governance well before systems are operational.

In the context of rural water governance, procurement is often carried out by entities with limited technical capacity and performance pressures. This is an environment conducive to the phenomenon that recent digital governance blogs have termed platform lock-in, whereby public authorities adapt their regulatory practices to the features of particular technological platforms, rather than seeking to influence the platforms themselves through law. Ultimately, this can lead to fragmented architectures in which different states or districts use different, indeed incompatible, platforms [66].

This is a nuanced but important change in the locus of regulatory power. With the regulation of data standards, models, and update cycles in the hands of private entities, the extent to which the state can influence the direction of regulatory policy is limited. Recent articles on digital public infrastructure have cautioned against the dangers of this model, where the result could be the emergence of a form of delegated platform governance in the place of democratic public governance, unless checked.

The absence of mandatory impact assessments of algorithms, transparency clauses, and exit strategies in public procurement contracts also increases the risk of AI systems outliving political cycles and policy priorities, effectively embedding particular regulatory logics into governance by default rather than by choice [67].

6.5 Exclusion, Algorithmic Legibility, and the Reproduction of Rural Inequality

One of the least discussed but most significant risks of AI-enabled governance is tied to its politics of legibility. In other words, AI systems function by breaking down complex social and ecological systems into standardised categories that a machine can read. However, recent work in critical governance theory highlights that such processes of legibility are inherently biased towards certain types of knowledge while excluding others. In the context of rural water governance, this creates a risk of reinforcing historical inequalities by systematically privileging regions, households, and practices that meet the data expectations of AI systems [67].

Recent development and policy issues have highlighted how digitally enabled governance systems have tended to privilege certain communities with good connectivity, administrative knowledge, and stable settlements. In contrast, seasonal migrant communities, informal settlements, and ecologically vulnerable regions have tended to be less represented in these data systems, making them less legible to AI systems that inform governance decisions. This lack of legibility will slowly translate into exclusion as governance becomes increasingly reliant on data-driven decisions to make priority interventions [68].

Apart from access and infrastructure, there are also epistemic forms of exclusion, which revolve around AI systems that use aggregated hydrological and consumption data and often ignore existing knowledge systems, water-sharing practices, and community adaptation mechanisms that have been developed to deal with ecological uncertainty. Recent blogs on participatory environmental governance argue that exclusion of knowledge systems not only undermines social justice but also undermines the effectiveness of environmental regulations, as they become less responsive to local variability.

From a regulatory governance perspective, there are deep and abiding concerns about democratic legitimacy. Environmental regulations that systematically fail

to recognize certain communities or knowledge systems cannot be seen to be fair or inclusive. The problem is not simply that certain groups or knowledge systems are excluded, but that exclusion becomes normalized through technical rationality, which remains sheltered from critical evaluation through claims to objectivity and efficiency. Without legal and institutional interventions to challenge these dynamics, AI could entrench a form of technocratic governance that, while formally rational, is substantively unjust [68].

6.6 Governing Risk Before Scale: Embedding Legitimacy in AI System Design

The above discussed analysis illustrates that the risks in AI-supported RWG are not circumstantial and dependent on effective implementation but rather inherent in the regulation by algorithm. Understanding risks in this manner is crucial for an effective legal response.

The theory of regulatory governance has long highlighted that effective regulation is not only dependent on the regulation's content but also on the institutional context in which the regulation is implemented. In the context of AI and RWG, the institutional context is defined in the design phase in which decisions on data sources, analytical tools, thresholds for intervention, and institutional responsibilities are programmed in the system design. Once programmed, they create a form of regulatory inertia that limits future legal and regulatory options [63].

An effective legal response to the risks in AI-supported RWG thus requires that the legal response moves from a post-regulatory to an ex-ante legal design. This means that legal frameworks need to articulate in advance the limits on data collection, allocation of responsibilities for algorithm-assisted decisions, and procedural rights for communities. In the absence of such articulation, algorithmic regulation risks operating as de facto regulators without legal authorization and accountability [68].

This design-oriented approach to understanding AI and its implications can also reshape how we think about efficiency and legitimacy. While AI systems can and should be justified on the grounds of their predictive accuracy and efficiency, regulatory governance research has argued that efficiency gains at the expense of transparency and contestability undermine long-term regulatory governance capacity. Regulatory governance systems that cannot be challenged, explained, or corrected risk generating resistance, judicial review, and institutional distrust. These would be highly destabilising effects in a rural water governance context in which legitimacy deficits already exist.

Ex ante legal design can also perform a distributive function in relation to AI and its implications. By requiring legal design to address questions of visibility and whose knowledge is relevant, law can address the risk that AI and algorithmic

systems will privilege standardised and data-rich contexts. This will be a significant consideration in a rural context in which there may be significant ecological and socio-economic variability [68].

In the final analysis, the governance of risk before scale is not about the restraint of technology, but is, rather, the very condition of sustainable innovation. AI can be used to improve the governance of rural water resources, but this is only the case if it is embedded in the legal framework that sustains the importance of accountability, inclusiveness, and control. This is the conceptual link to the next section, which looks at the possibilities of realizing these normative imperatives as institutional pathways for AI water governance in India.

7 Sustainable and Legally Viable Pathways for AI-Driven Rural Water Governance in India

Through the above discussions, the purpose has been served by establishing and confirming that artificial intelligence cannot be accepted or disapproved of as an important factor in governance and instability, respectively, independently as an administrative device or an agent of instability. The real value and significance of artificial intelligence regulation and its use as a tool pertain merely and more specifically to challenges of reconfiguring and reorganizing the present institutional landscape, as well as systems of authority and notions of legality, which becomes an important focus in dealing with the subject of this section.

7.1 Learning from Comparative Regulatory Models: Institutional Design as Opposed to Technological Sophistication

The regulatory viability of AI-enabled water governance is less a function of technological sophistication and more a function of authority and responsibility configuration as illustrated by its relative experience. Different jurisdictions have developed distinct regulatory architectures for AI-enabled water governance, shaped by different constitutional and governance cultures. Nevertheless, there is a degree of convergence around some design principles [69].

In a centralized model like Israel, where water is constitutionally a national resource, AI is implemented through a consolidated statutory authority with clear allocation, monitoring, and enforcement powers. In this model, AI-enabled monitoring is simply an extension of existing legal mandates and allows for a universal standard for data and real-time regulatory intervention. While this model is clear and coordinated, it also centralises power and responsibility within a single institution.

On the other hand, in Singapore, there is a system of statutorily regulated public utility governance in which AI is integrated. In this system of governance, smart water systems are fully legislated in terms of detailed regulations in relation to

AI-based monitoring in accordance with service standards and audit requirements. This example demonstrates how well-articulated law can ensure accountability in governance structures despite the data-driven approach.

The Netherlands has adopted a different approach in its system of polycentric governance in relation to AI-based water management systems in regional water authorities. In this system of governance, AI-based monitoring is used for predictive and preventive purposes in accordance with data sharing obligations and coordination between different levels of governance [69].

One common aspect of all the above systems of governance is the institutionalisation of data in its capacity as a regulatory tool rather than its usage as a mere product of technology. The comparative approach for India is not one of adopting the above systems but of adopting the design principles of such systems in a manner that can be adapted in the Indian context of multi-level governance in a democratically accountable system of governance.

7.2 Institutional and legal Pathways for India: Embedding AI within Democratic Water Governance

The translation of this understanding into the Indian scenario necessitates a consideration of the current legal architecture and the prevailing governance challenges. Rural water governance in India is marked by fragmented power structures, executive schemes, and local capacity gaps. In this scenario, the integration of AI has to be achieved through institutional embedding rather than parallel technological adoption.

- Firstly, adaptive regulatory structures are a prerequisite for the integration of AI in Indian water governance. While the current water and environment regulations offer normative mandates for water governance, there is a lack of specific provisions for data-driven governance. Rather than technology-specific regulations, a more sustainable route for Indian water governance could be the inclusion of enabling clauses in current regulations that provide for AI-based monitoring and decision-support systems with corresponding obligations of transparency, explanation, and review.

- Secondly, capacity building at the local level is essential. Panchayati Raj institutions hold a constitutionally important place in the governance of water in the rural area; yet, in the absence of local interpretive capacity building in the process of integrating AI, the chances of further centralisation of power and marginalisation of local voices are high. The theory of regulatory governance clearly indicates that decentralisation can be effective only through institutional competence.

- Thirdly, the process of public-private partnership should be governed through law rather than through contract-based relationships. While the

involvement of the private sector may be essential in the development of AI technology, the objectives of regulation should be clearly defined in the public domain. This can be achieved through the development of procurement policies that ensure interoperability, data ownership in the public domain, and audit trails of algorithmic systems.

- Finally, community participation must be institutionalized as an ongoing process of governance, not just a cosmetic exercise. New forms of decision-making and justification are being crafted by AI systems; thus, communities have to be able to query the accuracy of the data, dispute the results of the algorithm, and seek remedies. The institutionalization of grievance and review processes within the structures of AI-enabled governance ensures that regulation does not become technocratically isolated from the communities being regulated [70].

7.3 Reconciling Innovation with Legitimacy: Towards a Coherent Governance Paradigm

Collectively, these mechanisms imply that the sustainability of AI-based rural water governance is contingent on the ability of law to inform and shape technological rationality. Innovation and legitimacy are therefore not seen as conflicting values, but as complementary and mutually reinforcing values, contingent on the design of the governance system as a whole, balancing predictive capability with accountability and inclusion.

Regulatory governance theory highlights the point that legitimacy is not created by outcome, but by process, and that it must be intelligible, contestable, and just. For AI-based systems to be seen as improving the effectiveness of regulation, they must be embedded within such a process, and any efficiencies created by less transparent and more exclusive systems risk undermining long-term capability as trust is lost and resistance is mobilized [70].

In this respect, for India, the challenge is as much conceptual as institutional. That is, AI should not be conceived of as a solution for administrative shortcomings but rather as a driver for thinking differently about how environmental regulation is undertaken in an uncertain world [71]. Developing a framework for AI that is legal and institutional has the potential to transcend conventional reactive models of governance towards more anticipatory, inclusive, and resilient models of rural water governance.

This provides a backdrop for the final section of this paper, where there is a synthesis of the various legal and theoretical contributions that have been made and a reflection on the broader implications of AI as a form of regulatory enabler in environmental governance.

8 Conclusion

The above analysis shows that the legal issues involved within the AI-based water governance in the rural areas of India have numerous opportunities and challenges too. The issues are not only associated with the gaps in legislation but are also related to issues involving accountability and exclusion. The subsequent set of recommendations will offer a pathway for introducing the concept of AI within the governance of water resources, which not only takes advantage of the latest technologies in regulation but also finds inspiration from the theories and regulation from various parts of the world.

a. *Legal Recognition and Accountability Frameworks for AI in Water Governance*

Problem: Obviously, the use of the AI systems in the water governance process is often not accompanied by an explicit legal status and accountability design, creating issues regarding the responsibility of determinations resulting from the use of predictive analytics/monitoring.

Solution: Create legal requirements that include and integrate AI systems effectively within water governance systems. These requirements include the legal bases for the use of AI systems, the responsibility of water administrators, and that for explainability. Therefore, by integrating AI systems with water governance laws, it opens the way for the use and application of AI systems to classic decision-making processes; by doing that, it becomes feasible to utilize AI for legal purposes without violating any laws. It also reduces the risk of a decision being made without a reason, as decision-making without a reason invites liability for adverse consequences.

b. *Mandatory Data Governance Standards for Public Sector AI*

Problem: AI systems must be fed high-quality, representative data, but increasingly, in the public sector, there are problems with poor data quality, fragmentation, or a lack of governance, resulting in bias, exclusion, or even poor predictions.

Solution: Legally binding requirements are necessary for the data quality, interoperability, provenance, and access aspects of AI-enabled governance. Data governance models include data collection, storage, sharing, and auditing; therefore, data should meet the overall requirements of data accuracy, completeness, and fairness before applying AI systems. This enhances reliability and accountability and is consistent with an overall public sector approach that focuses on AI governance in terms of its relationship with the concept of fairness and other transparent aspects of the overall AI lifecycle.

c. *Institutionalised Participatory Mechanisms for AI-Enabled Regulation*

Problem: There is the possibility that AI may actually end up marginalising some communities due to a lack of participation and transparency when decisions are made over resources and triggers.

Solution: Integrating a participatory component within the 'rules of the game' of AI in water governance. This is achieved through co-design, feedback, and rights to contest AI decisions. Studies on AI in water governance emphasize the role of participation of citizens, along with the development of appropriate norms and ethical parameters, in responsible governance, avoiding technocratic exclusion (Participatory AI literature).

d. Institutional Capacity Building and Digital Inclusivity Mandates

Problem: Marginalised and rural societies frequently lack the digital infrastructure, literacy, and attendant systems required for effective engagement with, intervention in, and/or benefits from AI-driven water governance.

Solution: Develop legislation on the mandate for capacity building and digital inclusion that supports local institutions in engaging with AI systems. In line with the literature on the challenges public sector organizations experience in AI adoption, the government can invest in the development of skills and interpretive capacities that support the meaningful engagement of the local institutions in AI governance, ensuring that AI does not become an elite tool accessible only by those with the ability to afford it, but a public space of regulatory engagement and participation.

e. Ex Ante Risk and Impact Assessments for AI Deployment

Problem: The risks posed by AI are not necessarily accounted for within existing structures of governance, as the technology can pose unforeseen harms prior to regulatory adaptation; existing regulatory frameworks often fail to require the evaluation of socio-legal and environmental risks prior to use.

Solution: Mandatory ex ante risk and impact assessments could be built into the legal framework before the use of AI systems in RW management. Ethical, social, legal, and environmental impacts could be considered in these assessments, which should include independent assessment mechanisms. These assessments thus align with the notion of an emergent model of hybrid governance concerned with risk management across the lifecycle of AI systems, sometimes also called AI governance systematic review.

Needless to say, the paper has also emphasized the need to consider AI not only as an emerging technological solution, but also as an emerging mode of regulation in the rural water governance architecture itself. Thus, as a solution for monitoring, predictive analytics, or even decision support, AI can certainly be seen as addressing the historic challenges related to issues like water scarcity, water quality, and infrastructure performance. With regard to the actual governance issues, however, its implications extend well beyond those of

efficiency or effectiveness into important questions of regulatory fragmentation, etc., in India.

By utilizing a regulatory framework of governance, along with a techno-legal perspective, and learning from comparative experiences in country-specific contexts that have been implemented in Israel, Singapore, and the Netherlands, the paper seeks to exemplify how AI enables regulatory governance. However, such a phenomenon can only be achieved in a manner that seeks a conjunction with legally sound architectures. Inasmuch as such a lesson can be learned and implemented in the Indian context, there exists a need to shift from a policy-driven model to a legally derived perspective that seeks the inclusion of AI-developed results assisted through decision-making instruments.

Ultimately, it is a position that sustainable management of rural water supplies cannot be accomplished by means of technology adoption; rather, it was crucial that legal regulation and constraint/limitation of AI development would enable it to play an efficacious role for democratic governance. Thus, there exists a human necessity for a congruence between law and technology that does not only capitalize on the potential for technology use within a body of regulation but also capitalize on the potential for development within a body of regulation and for development itself.

Acknowledgment

The authors would like to express their sincere gratitude to University of Engineering and Management Kolkata for providing the necessary academic environment, infrastructure, and support to carry out this research work successfully. Also, a grant-in-aid of around INR 15,000 was allocated for this project from the University. The authors also acknowledge the Department of Law, University of Stockholm for active collaboration.

Contribution of each Author

Abhisikta Basu has conceived the idea of the paper and did the initial drafting. Avishikta Chatterjee has done the comparative analysis of the various countries. Debargha Kundu has done the case analysis in the Indian perspective.

Conflict of Interest Statement

The authors declare no conflict of interest.

References

1. Government of Israel, Water Law, 1959.
2. Republic of Singapore, Public Utilities Act, 2001.
3. Government of the Netherlands, "Water management," 2025.
4. S. Russell and P. Norvig, Artificial Intelligence: A Modern Approach, 4th ed., Pearson, 2021.
5. I. Fadel and V. A. Tzanakakis, "AI in water resources," *Environmental Modelling & Software*, 2017.
6. A. Mosavi et al., "Flood prediction using ML," *Water*, 2018.
7. K. Yeung, "Algorithmic regulation," *Regulation & Governance*, 2018.
8. E. Fisher et al., *Environmental law*, 2nd ed., Oxford Univ. Press.
9. S. Zouridis et al., "Algorithmic decision-making and law," *Public Administration Review*, 2020.
10. C. Busch, "Algorithmic accountability," J. European Consumer Law, 2022.
11. A. Richards and N. Singh, "Water and federalism: India's institutions governing inter-state river waters," UC Santa Cruz Dept. Econ., 2000. [Online]. Available: https://people.ucsc.edu/~boxjenk/waterdom.pdf
12. (1991) 1 SCC 598.
13. *Subhash Kumar* v. *State of Bihar*, (1991) 1 SCC 598.
14. (1999) 2 SCC 718.
15. (2000) 10 SCC 664.
16. (2001) 6 SCC 496.
17. Government of India, The Water (Prevention and Control of Pollution) Act, 1974.
18. A. Tahir and A. Visaria, "Sewage pollution in water supply in Indore," Indian J. Occupational and Environmental Medicine, vol. 21, no. 3, p. 149.
19. T. Schellenberg et al., "Wastewater discharge standards in the evolving context of urban sustainability – The case of India," Frontiers in Environmental Science, vol. 8, 2020.
20. Ministry of Jal Shakti, "Demand No. 62: Department of Water Resources, River Development and Ganga Rejuvenation," Union Budget of India, 2024. [Online]. Available: https://www.indiabudget.gov.in
21. J. Kothari, "The right to water: A constitutional perspective," 2009. [Online]. Available: https://www.ielrc.org
22. Department of Drinking Water and Sanitation, "Assessment of employment generation potentials of Jal Jeevan Mission," Ministry of Jal Shakti, 2023.
23. Sustainable Policy Research Foundation India, "Indian agriculture: Policies for sustainable transformation," 2021.
24. Finance Commission of India, "Law and economics of the third stratum," 2023.
25. C. Shen, "Deep learning in water science," Water Resources Research, 2018.
26. M. Satishkumar et al., "AI and IoT in water management," J. Hydrology, 2021.
27. Government of Israel, "National water efficiency report," Israeli Water Authority.
28. Israeli Ministry of Energy and Infrastructure, "Water Authority – Roles and responsibilities."
29. NoCamels, "Israel's national water carrier installs AI monitoring," 2023.
30. Public Utilities Board, "Water quality and safety," Singapore Government.
31. Public Utilities Board, "Smart water meter programme," Singapore Government.

32. MDPI, "Smart water grids and digital governance in Singapore," Water, vol. 17, no. 13, 2024.
33. Government of the Netherlands, "Water management in the Netherlands."
34. Dutch Water Authorities, "The Dutch water authority model," 2021.
35. OECD, "Water governance in the Netherlands: Fit for the future?" 2014.
36. Rijkswaterstaat, "About Rijkswaterstaat," Government of the Netherlands.
37. ResearchGate, "Water governance in the Netherlands," 2023.
38. Government of India, The Water (Prevention and Control of Pollution) Act, 1974.
39. Government of India, The Environment (Protection) Act, 1986
40. S. Singh and M. K. Goyal, "A review of India's water policy," J. Water and Climate Change, vol. 16, no. 2, pp. 493–510, 2025.
41. U.S. Geological Survey, "Real-time water quality."
42. KPMG, "Harnessing AI to reimagine water governance in India," 2025.
43. RIKA Sensor, "Why IoT is used in real-time water monitoring," 2025.
44. K. Saravanan et al., "Real-time water quality monitoring using IoT," Environmental Monitoring and Assessment, vol. 190, 2018.
45. J. Zalte and H. Shah, "AI-driven predictive analytics for disease detection," 2025.
46. N. N. M. Rizal et al., "Water quality predictive analytics using ANN," Water, vol. 14, no. 8, 2022.
47. Prism Sustainability Directory, "Predictive analytics in water quality management," 2025.
48. V. Vivek et al., "Planning for India's rural drinking water," USAID, 2024.
49. Swedish Law Study, "Integrated governance of freshwaters."
50. G. Mathew et al., "Decentralisation and democratic governance," 2003.
51. C. Li, "AI-driven governance," Digital Society & Virtual Governance, 2025.
52. E. M. Amine, "Impact of AI in water governance," E3S Web of Conferences, 2025.
53. D. Ddiba et al., "Governing circular economy," Earth System Governance, vol. 4, 2020.
54. C. Orwat et al., "Normative challenges of AI regulation," NanoEthics, 2024.
55. National Economic Forum, "India's AI regulation strategy," 2025.
56. Agenda 2030 Blog, "Can AI solve environmental challenges?" 2023.
57. C. Ducuing, "Data as infrastructure?" Competition and Regulation in Network Industries, 2019.
58. RTI International, "AI data center infrastructure," 2025.
59. Prism Directory, "Ethical data governance," 2025.
60. A. Gaidartzi and I. Stamatoudi, "AI authorship issues," Laws, 2025.
61. P. N. Ma'rifah et al., "Smart digital water monitoring," Jurnal TRIAC, 2025.
62. H. Tripathi, "Right to privacy in the digital age," 2024.
63. P. Balboni and K. E. Francis, "Data ethics and sustainability," Journal of Responsible Technology, 2024.
64. NICE Actimize, "Ethics of AI in surveillance."
65. D. M. R. K. M. Agarwal, "AI in environmental monitoring," Zenodo, 2025.
66. C. Castelluccia and D. Le Métayer, "Algorithmic decision-making," European Parliament, 2019.
67. T. Kulkarni, "Water governance challenges," J. Eng. Applied Sciences Tech., 2022.
68. S. Bilalova et al., "Paradigms of water governance," Ecology and Society, 2026.
69. L. Colonna and S. Greenstein, Nordic Yearbook of Law and Informatics, 2022.
70. D. Vekaria and S. Sinha, "aiWATERS framework," AI in Civil Engineering, 2024.
71. J. G. Allen et al., "Singapore's AI governance," 2025.

Abhisikta Basu is a legal researcher at the Department of Law (IIIJS), University of Engineering and Management, Kolkata. Her work focuses on the intersection of law, technology, and forensic applications, with particular interest in AI governance, digital evidence, and evolving legal frameworks in complex investigative contexts. She has a growing academic profile with multiple citations and is actively engaged in interdisciplinary research bridging legal studies and scientific innovation.

Avishikta Chatterjee is a legal researcher specializing in environmental law sustainability, and policy. She is currently pursuing an LL.M. in Environmental Law at Stockholm University and holds a BBA LL.B. (Hons.) with a specialization in Corporate Law. Her work focuses on the intersection of law, environmental governance, and public policy, with particular interest in ESG frameworks, corporate accountability, and sustainability transitions. She has authored multiple publications in Scopus-indexed journals and is actively engaged in interdisciplinary research, including quantitative legal analysis of corporate environmental impacts.

Debargha Kundu is a law student pursuing B.B.A. LL.B. (Hons.) with a specialization in Corporate Law from the University of Engineering & Management, Kolkata. His interests lie in corporate, competition, and intellectual property law. He has gained practical experience through internships with institutions such as the Competition Commission of India and Fox & Mandal, where he worked on legal research, drafting, compliance, and arbitration matters. He has also contributed to legal scholarship through publications in corporate and IPR law, and has actively participated in moot court competitions, securing notable achievements including a national-level win and a Best Speaker award.

Interdisciplinary Journal of Computing & AI

IJCAI
Interdisciplinary Journal of Computing & AI

IJCAI

RESEARCH

Privex: A Privacy-Preserving Online Meeting System Using Hybrid Cryptography

Tiyasa Paul[1*], Rohan Samanta[2], Pratik Saha[3], Partha Pratim Chaulia[4], Sudip Kumar Palit[5]

[1,2,3,4,5]*Department of Computer Science and Engineering (Artificial Intelligence & Machine Learning), Institute of Engineering and Management, University of Engineering and Management, Kolkata, West Bengal, India*
[5]*Cybersecurity Centre of Excellence, Institute of Engineering and Management, University of Engineering and Management, Kolkata, West Bengal, India*

Email: [1]shreetiyasa2003@gmail.com; [2]rohansamanta56@gmail.com; [3]pratiksaha964@gmail.com ; [4]prarthapratimchaulia@gmail.com; [5]sudipkumar.palit@uem.edu.in

ARTICLE INFO.

Keywords: End-to-End Encryption, Authentication, Non-Repudiation, Multi-Session Management, Co-Host Delegation, Message Automation

*Corresponding author email address: shreetiyasa2003@gmail.com

Manuscript received: 21 January 2026/Accepted April 10 2026
Published online: 17 April 2026
https://doi.org/10.5281/zenodo.19627442

Cite as: T. Paul, R. Samanta, P. Saha, P. P. Chaulia and S. K. Palit, "Privex: A Privacy-Preserving Online Meeting System Using Hybrid Cryptography", Interdisciplinary Journal of Computing & AI (IJCAI), vol. 1, no. 1, Aspiration Publishing Trust (DARPAN ID: WB/2025/0887371), p. 122-161, Apr. 2026, doi: 10.5281/zenodo.19627442.

ABSTRACT

In this paper, a behaviour-sensitive session orchestration architecture over secure communication and the rationale behind it will be proposed and discussed, which is a variant of mixed public-key cryptography that aims at offering more manageable, secret, and authenticity in real-time messaging infrastructure. The architecture incorporates the use of RSA and Diffie Hellman in ensuring the setup of user sessions and relies on AES to encrypt instantaneous messages very quickly. Multi-fernet algorithm supports the distribution of session keys and ensures that the key is recovered by the authorized parties only. There are also digital signatures based on RSA that facilitate authentication and non-repudiation but strong hash algorithms are applied to ensure the privacy of user passwords. The system has collaborative features along with cryptographic protection, including co-host delegation, active user blocking, permissions and multi-session to support multi-user logins. Also, the design

enables the dynamically updating of the authentication credentials without disruption of the existing communication. The suggested hybrid configuration has a higher level of defense against cryptographic attacks and unauthorized access than single algorithm implementations, which is why it is a more robust and secure solution. In conclusion, the provided solution contributes to the fact that the process of communication in the environment of multi-users becomes much safer, convenient, and manageable.

1 Introduction

Nowadays, as digital messaging is being delivered throughout the world, securing information being transferred over unstable, publicly available networks is a challenge in security studies. The methods such as RSA are useful in upholding privacy, accuracy and verification by use of encryption and signatures, but they are not always flexible. This algorithm helps to prevent the service disruption as well. In the meantime, the Diffie-Hellman method allows two parties to establish shared keys in a secure manner -even before prior coordination. Nevertheless, traditional methods are mostly ineffective in rapidly evolving circumstances when it is necessary to involve a group of users who need more intense control. The approach to public key enhances security and convenience by connecting RSA and Diffie-Hellman characteristics. Verified identities are used to create secure channels of chat with the help of hashed login information. Origin evidence is stored through digital marks through RSA. Even more, added functionalities were used to meet the real teamwork needs. Several sessions are supported and the host rights can change to co-host during a meeting. System alerts can be automated where limited to a constraint where password updates are still secured where it remains in active communication. The result of such upgrades is an increased flexibility throughout common cyberspace. The method employs concepts of various encryption systems to address vulnerabilities in individual systems, but enhance defence to common attacks. The testing was carried out in modelled environments in order to check on the safety measures as well as speed with varied hacking efforts. The following sections will discuss set up design, obstacles during the construction, and trial results with a combination of examples. It has been found that the model enhances teamwork tools over the internet without slowing down or complicating their use. It combines a variety of simultaneous sessions, shared hosting privileges, auto-messages can be disabled, denying any action is not possible and lets the user change their password safely on the same idle session. In contrast to the earlier models, which relied on one technique, this strategy can stand threats more efficiently, but change to various scenarios more readily.

2 Literature Survey

Considerable effort has gone towards developing both secure communication systems and cryptographic frameworks that enable the secure transfer of digital data between parties over a public channel. The current literature is able to be grouped systematically within five main research trajectories: (i) Secure communication and End-To-End Encryption (E2EE) (ii) Cryptographic Key Management and Exchange Protocols (iii) Integrity and Authentication of messages; (iv) Comparative Analysis of Hybrid Cryptographic Architectures; and (v) 5 Domain-Specific Security Architectures. A summary comparison of the different approaches on the basis of their security characteristics is included in Table 1.

2.1 Secure Communication and End-to-end Encryption

Numerous publications have been created to reduce weaknesses in validation using more advanced (and hybrid) encryption techniques and methods. Asha Jerlin *et al.* [1] have proposed an architecture for secure messaging using both RSA and AES (advanced encryption standards) to ensure data's confidentiality and the integrity of the message. Likewise, Almaiah *et al.* [2] developed a hybrid method combining elliptic curve cryptography (ECC) and Hill cipher-type systems to increase the security of mobile data transmissions from 'eavesdropping' or 'interception' threats. Likewise, Sivakumar et al. have developed a safety system for cloud-based communications using AES-RSA Hybrid Encryption combined with QKD (quantum key distribution) to ensure a 'future-safe' key. In addition, Fouzar *et al.* [3] have developed an ECC-based Hybrid Algorithm that is optimised for secure video streaming, which uses dynamic key scheduling in order to encrypt multiple video segments individually and to prevent unauthorised access to these segments. All of these studies demonstrate that hybrid cryptographic primitives successfully provide communication channels with robust protection from cyber-attacks.

2.2 Cryptographic Key Management and Exchange Protocols

The reliability of cryptographic systems highly relies upon good mechanisms for generating and distributing keys. To overcome the difficulties involved with transferring keys securely, Lein Harn *et al.* [4] created a decentralized way to establish a group key using mechanisms based on Diffie-Hellman functions and secret sharing instead of a central location (KGC) to generate keys. For cloud computing, Ahmad *et al.* [5] created an HCA-KMS (hybrid ECC and AES Key Management System) to assist with the management of cryptographic materials throughout their lifecycle in a virtualised environment. In addition, Sivakumar *et al.* [6] suggested the introduction of quantum key distribution (QKD) to strengthen the security of the key exchange process from quantum-based attacks. All of the methods discussed

here indicate that scalable and robust Key Management Systems (KMS) are essential to maintain the integrity of existing communication systems.

2.3 Integrity and Authentication of Messages

The security of today's communications infrastructures is fundamentally reliant upon two critical components: entity authentication and data integrity. To meet these needs, Asha Jerlin *et al.* [7] provide an integrated approach using the Diffie-Hellman protocol for a secure key exchange and session establishment, along with the Elliptic Curve Digital Signature Algorithm (ECDSA) and HMAC-SHA512 for message authentication and data integrity check upon receipt. Ahmad *et al.* [5] have also proposed a hybrid architecture to protect against impersonation attacks in the verification of entity-to-entity transactions that incorporate layered authentication in the cloud computing environments. Collectively, these approaches promote non-repudiation and also guarantee the integrity of data while it is being transmitted, forming a verified trust relationship between participants involved in communication.

2.4 Comparative Analysis of Hybrid Cryptographic Architectures

The synergy of symmetric and asymmetric cryptographic primitives has received much attention through extensive research efforts to optimize security and performance in secure online transactions and communication protocols. In their work analyzing hybrid cryptographic frameworks by Bhatele *et al.* [8], a detailed taxonomy was developed. The authors describe the basic premise of the hybrid methodology as follows: the symmetric algorithm provides computationally efficient processing of large quantities of data with high throughput; the asymmetric algorithm provides an additional layer of security for digitally signed messages and other types of electronic transactions by securely distributing robust keys that can be used to encrypt and decrypt data. By incorporating both methodologies into a single framework, hybrid systems are capable of providing higher security levels and greater data confidentiality, while at the same time maintaining low levels of latency and/or overhead within existing modern telecommunications networks.

2.5 Domain-Specific Security Architectures

Recent studies have focused on adapting cryptographic primitives to solve the unique constraints created in heterogeneous network types. An example of this would be Almaiah *et al.* [2], who developed a hybrid encryption scheme to make it more difficult for hackers to breach mobile communication protocol weaknesses due to wireless data transmission. Also, Fouzar *et al.* [3] implemented hybrid cryptographic architectures in multimedia streaming systems to provide the greatest data confidentiality and the lowest possible latency for real-time traffic. Both implementations show that there are

scalable cryptographic frameworks that may be customized to fit different application layer security demands.

2.6 Research Gap

When looking through the reviewed literature, we will see that there are many individual security solutions available such as encryption schemes, key management schemes, authentication schemes, or hybrid cryptographic schemes. Most of these solutions do not type in these components together to create one successful secure communication platform but tend to separate the elements out creating an unclear picture of what makes up a secure communication platform. The specified constraint of creating a solution with end-to-end encryption, non-repudiation, dynamic access control and secure session management added to the urgent need for the Privex system to exist. Table 1 represents the comparison of cryptographic techniques based on security and performance parameters is presented.

3 Proposed Approach

To ensure the safety, privateness, and reliability of communication in the app, a unique message and session system was created. Since it conforms to the basic requirements of security like secrecy, accuracy and accessibility, it is also useful in demonstrating the action taken in a court of law. Using such a structure, people can post information safely, authenticate themselves with whom they are communicating, can revoke permissions, block intrusions, altered posts, and bogus rejections at any time to come. Here a hybrid encryption strategy is adopted. To provide better key management and encryption of messages, the system uses multi-Fernet, which is a symmetric encryption utility that is offered by the cryptography package of Python. Each interviewee provides its own AES key, with which the multi-Fernet framework manages and merges to create a single master key. All session messages are then encrypted using this master key. This key cannot be accessed by anyone but an authorized user.

Privex uses a Server-Assisted End-to-End Encryption trust model, in which session messages are fully AES-encrypted at the endpoint of the sender and never leave the device, so the server is implemented as a ciphertext relay, and does not understand any content of the session messages at all - even a completely compromised server cannot read session messages. The session AES key is also secured by Multi-Fernet construct in which all the authorized participant key-shares are necessary to rebuild it and hence no one breach is possible on the server-side. The private keys of the RSA are stored in encrypted format only on the server, and they are encrypted over AES-128-CBC using a key derived with the personal password of the user via scrypt - a memory-hard algorithm that is difficult to brute force. The password used by the user is never stored or sent to the server in decipherable form and this

ensures that the server is the holder of the locked box but does not possess the key to unlock it.

Table 1 Comparison of cryptographic techniques based on security and performance parameters

Paper / Approach	Encryption Type	Security Features	Runtime Performance	Time Complexity
Ahmad et al. [5]	Hybrid (ECC + AES)	Confidentiality, Integrity, Key Management, Authentication, Secure Cloud Storage	Very High (Optimized ECC Keys)	O(log n)
Almaiah et al. [2]	Hybrid (ECC + Symmetric Hill)	Confidentiality, Authentication, Keyless Exchange, Secure ASCII Mapping	Moderate	$O(n^2)$
Jerlin et al. [1]	Hybrid Symmetric-Asymmetric	Confidentiality, Integrity, Authentication using AES + RSA, JWT for Login	High (AES-based)	$O(n^2)$
Lein Harn et al. [4]	Hybrid Diffie-Hellman	Key Authentication, Key Independence, Confidentiality	High	O(n)
Sivakumar et al. [6]	Hybrid + Quantum Key Distribution	Confidentiality, Integrity, Secure Key Sharing, Cloud Data Security	High (Cloud Computation Overhead)	$O(n^3)$
Bhatele et al. [8]	Hybrid (Symmetric + Asymmetric)	Integrity, Confidentiality, Authentication	Moderate	$O(n^2)$
Fouzar et al. [3]	ECC+Multi-Key Hybrid	Dynamic Keying, Multi-Layer Encryption, Anti-Piracy	High (Android Implementation)	O(n log n)

This hosted-key architecture is not a security compromise, but is intentional. Attributes that are core to the contribution dynamic cryptographic access revocation, co-host delegation, live key rotation and session-safe password updates need the server to actively participate in the key management

coordination, which is architecturally impossible with a pure zero-trust, device-local-key model. Privéx cryptographic architecture is specifically designed in a manner that all the sensitive operations message confidentiality, session key protection, and private key security are specified by mathematics and user-controlled credentials only, such that the system security assurances are universally true irrespective of the role played by the server in the communication process.

Decryption is carried out at the local level, i.e. end-users decrypt the data using renewed keys. This method guarantees privacy of information at every transfer level. When a user enters, exits or is removed out of a certain session the main key is updated dynamically, i.e., old access is no longer possible, but protection to new access is not compromised. The security is sensitive to the transforming conditions that are automatically rekeyed - continuity with exposure. The use of two-level RSA encryption may be appointed to offer non-repudiation - not repetition-based but a structural-check. Every user is given a single RSA key pair which is composed of a portion that is private and the other one is public. Privacy layer is ciphered with a password-based cipher and is stored in the server; others on the other side can however access the public one when communicating. When one logs in, he or she is decrypted using his or her passphrase of the user and the secret key is loaded into a temporary run time memory. This stored personal information is manifested in the tagging of the active and outgoing messages with a digital stamp when they are in use. When receivers get them, they validate the mark with a counterpart that is obtainable in the open of the broadcaster. Such validation ensures that every object dispatched is always closely tied to its place of origin - eliminating future arguments of non-involvement. This contract supports predictability of law suits in which evidence is a matter of count.

A live blocking tool was created in a manner that enables hosts to have control of hosts when they are in open meetings. The method relies on the Diffie-Hellman to come up with temporary secret keys between the host and the attendees. When one gets blocked, a number of things happens at the same time; a system issues a blocked flag in the database, issues new key sets to non-blocked people, and pulls the primary session key. Thanks to this fact, the excluded person will be unable to use his/her old key any more - the information on the access to the cache is automatically vacated. Any attempt by the blocked user to rejoin is rejected instantly as at the encryption level there are invalid. In addition to providing a superior privacy and control, the design enables rapid updates and stable sessions in case of a group work. The security is improved through using HTTPS connections, encrypted login codes, and HMAC authentication of the trust of the sessions and managing the active states with Flask and Flask-Socket IO. On a cumulative basis, the methodology creates strong, scalable security, which satisfies the current regulations of safety and which adjusts to the evolving requirements in the common digital landscapes with ease.

Figure 1 presents the flowchart of the proposed approach, illustrating the backend meeting initiation process, dynamic blocking mechanism, and secure key establishment using RSA and Diffie–Hellman. It shows how clients are authenticated, access is controlled through block and key verification, and session security is maintained by regenerating shared keys whenever user participation changes.

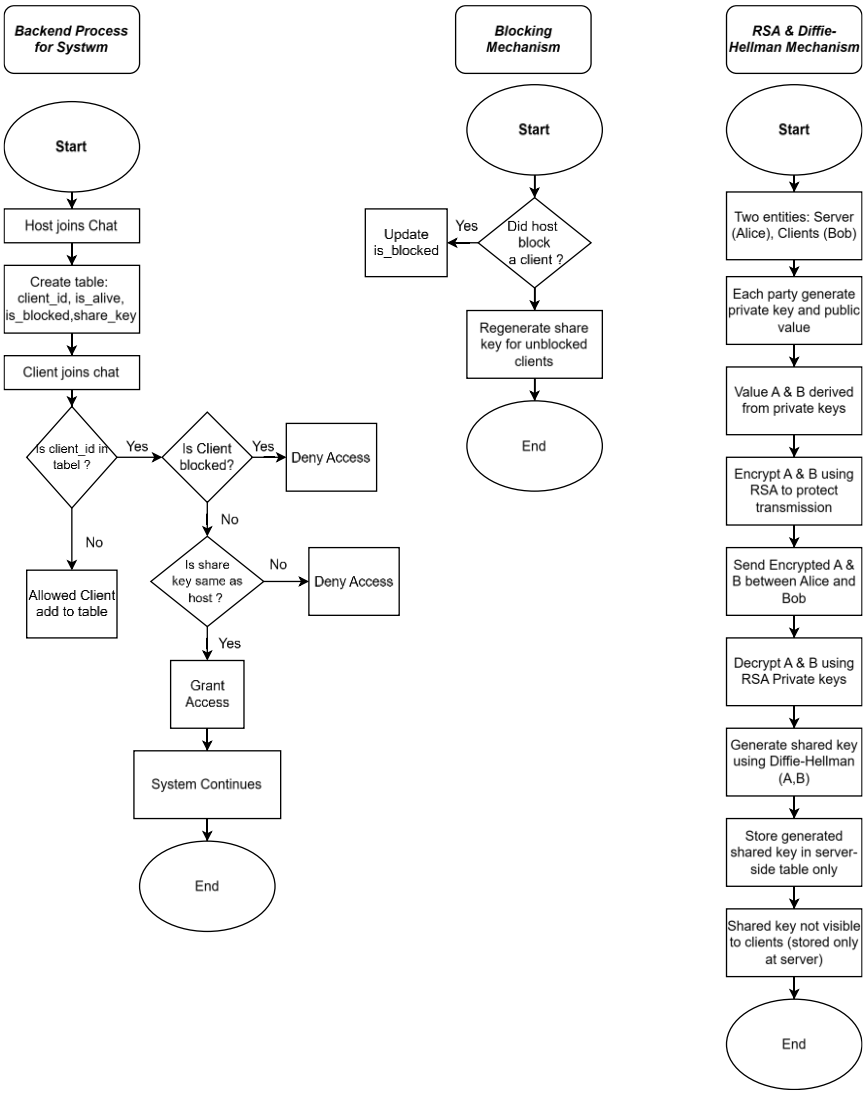


Fig. 1 Flowchart of Proposed Approach

3.1 Implementation of Proposed Approach

The proposed secure communication architecture is built around a modular, protocol-based Python architecture, which is heavily customized on the Flask web framework and Flask-SocketIO to handle real-time sessions. Flask session-based authentication is utilized to carry out user authentication and session management with user credential safely processed using hashlib module with hash-256 hash and stored in SQLite database. The communication between the client and server is fully carried out by means of HTTPS (TLS), which offers safe encryption of the transport-layer. Live meetings are dynamically controlled by the backend which manages active state of sessions, user roles (host/co-host/participant) and access permissions, making it possible to fine-tune live meetings.

The hybrid symmetric-key made on the basis of Secret Sharing and cryptography Python module are used as an end-to-end encryption technique. The generation of individual AES keys per participant with the assistance of the Fernet scheme is used in each meeting session. These keys along with purpose are combined using a Multi-Fernet construct whose purpose is a secret-sharing layer disclosing a master encryption key with no corresponding plaintext. The master key is used to encrypt AES key with all the message content which is session specific. The encryption and decryption are performed at the client-end point alone hence, actual end-to-end confidentiality. Every time a participant joins, leaves or gets stuck, the system triggers an automatic key rotation scheme which reconstructs participant keys and re-encrypts the session key in such a way as to provide both forward and back secrecy without stopping the running session.

Non-repudiation and access control can be enforced by using public-key cryptography and key management. The creation of key pairs of RSA via Crypto. Public Key, RSA, as well as the encryption of the private keys with the help of password-based key derivation (scrypt with AES-128-CBC) and subsequent secure storage, is done. Messages sent are digital- signature signed with the RSA private key of the message sender and authenticated at the receiver side by the RSA public key which in turn is authenticated by the SHA-256 hash function with the PKCS1 authentication signature. Traceability All the signature and verification process is logged to append-only audit files. This is done through a dynamic blocking algorithm that runs on Diffie-Hellman key exchange protocol whereby shared secrets are re-computed each time a user is blocked. This invalidates the old session keys and tokens accumulated before and invalidates them all at once thus preventing unauthorized re-entry or decryption of messages. Co-host delegation further enhances availability because it supports a tying together of session control delegation so that the continuity and security of collaboration can be maintained throughout the meeting life cycle.

3.2 Algorithms

3.2.1 End-to-End Encryption Algorithm

The encryption plan proposed will protect chat data between the participants in a mixed AES key-based set-up. In a Multi-Fernet model where each user is given a unique key of AES that is re-generated each session, keys are concatenated so as only the authorized users will be able to recombine to get the original decryption key. This primary key, in its turn, freezes a new AES session key, whereas the same AES session key codes all messages sent during the meeting. This is called end-to-end encryption because the AES key that is used to encrypt a message is not known to the servers and middle systems. The decryption rights are only granted to the verified users on both sides, therefore, the only people that can unlock the content. Information is encrypted as it passes and it is only relayed by the node without access tools. Thus, once the attackers are getting access to the internal systems, logs or in personnel assistance, secrecy is maintained. The layer is the most significant one in case of virtual meetings when personal talks, financial papers or personal communication should better remain beyond the reach of the unwary persons. The implication of this is that keys are re-used when an individual joins or leaves a session such that the previous participants cannot decrypt the following messages (forward secrecy), and the new ones cannot read the previous messages (backward secrecy). Whenever such an update is done, new keys are invented automatically and swapped on ensuring that the level of protection is high even when the groups are swapped frequently. No security is lost that slows down performance. The core end-to-end encrypted message in the Privex system, which is used to safeguard all the communications that occur during meetings is described in the Pseudocode 1. Through it, the messages are encrypted and decrypted by authorized members only and the server is used as a relay and has no access to plaintext messages. The algorithm uses dynamically regenerating cryptographic keys when the membership of the participants varies thus maintaining the confidentiality as well as forward and backward secrecy all through the meeting lifecycle. This same end-to-end encryption and key regeneration process is illustrated in Figure 2.

Pseudocode 1 End-to-End Encryption

```
Initialize E2E Encryption Module
FUNCTION E2E.initialize()
 Generate AES keys for all users in a meeting
FUNCTION create_AES_keys_for_users(users, meetingId)
FOR each user IN users DO
key ← Generate random Fernet key
STORE key in MeetingKeysDb(user, meetingId)
END FOR
```

```
9.  End function
10. FUNCTION get_master_key(meetingId)
11. keys_list ← FETCH all keys from MeetingKeysDb USING
    meetingId
12. master_key ← MultiFernet(keys_list)
13. RETURN master_key
14. End function.
15.  FUNCTION set_Aes_key(meetingId)
16.  plain_key ← Generate new Fernet key
17.  master_key ← get_master_key(meetingId)
18.  encrypted_key ← Encrypt(plain_key, master_key)
19.  STORE encrypted_key in MeetingAES(meetingId)
20. End function
21.  FUNCTION format_key(meetingId, users)
22.  encrypted_key ← FETCH encrypted key FROM MeetingAES
23.  master_key ← get_master_key(meetingId)
24.  decrypted_key ← Decrypt(encrypted_key, master_key)
25.  CALL rotate_keys(meetingId, users)
26.  new_master_key ← get_master_key(meetingId)
27.  re_encrypted_key ← Encrypt(decrypted_key, new_master_key)
28.  UPDATE MeetingAES with re_encrypted_key
29. End function
30.  FUNCTION encrypt(msg, meetingId)
31.  encrypted_key ← FETCH encrypted key FROM MeetingAES
32.  master_key ← get_master_key(meetingId)
33.  actual_key ← Decrypt(encrypted_key, master_key)
34.  ciphertext ← Encrypt(msg, actual_key)
35.  RETURN ciphertext
36. End function
37.  FUNCTION decrypt(token, meetingId)
38.  encrypted_key ← FETCH encrypted key FROM MeetingAES
39.  master_key ← get_master_key(meetingId)
40.  actual_key ← Decrypt(encrypted_key, master_key)
41.  plaintext ← Decrypt(token, actual_key)
42.  RETURN plaintext
43. End function
44.  FUNCTION rotate_keys(meetingId, users)
45.  DELETE existing keys FROM MeetingKeysDb USING meetingId
46.  CALL create_AES_keys_for_users(users, meetingId)
47. End function.
48. End.
```

3.2.2 Non-Repudiation Using RSA Digital Signatures Algorithm

This system may support non-repudiation property whereby each message sent during a given session is linked to a real source in a secure manner where the parties concerned will not be able to denounce the involvement.

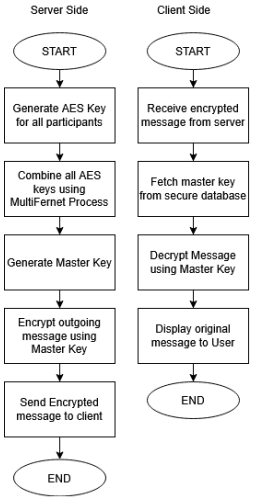


Fig. 2 Flowchart of End-to-End Encryption

The lack of ability to complain later that a message was not written or sent by the user is that since messages contain the transmissions of the digital signatures that are signed with a private key, the association between an individual and a message can resist verification. The latter plays a crucial role in the secure messaging arrangements, particularly in the team work where the sense of responsibility is observed, as the latter grants the monitoring of the actions, as well as the reliability of the latter. This is what has been termed as non-repudiation since the process could not be repudiated by the cryptographic evidence which is directly linked to the individual. To achieve this, users create own RSA key pairs upon registration.

In storage, the private key is encrypted by a password mechanism - that is, scrypt with AES-128-CBC - which is only decryptable by the owner at a later stage. Quite to the contrary, the public key is shared by free means and the digital signatures can be verified by other people. In order to send passwords, the source cannot only compute a SHA-256 digest of the original text, but he or she signs with his or her own secret key and he or she adheres to the PKCS1 v1.5 protocol. Together with this cryptography evidence, additional information about who sent it, the time, and the session identifier are recalled as one and creates an indelible trace that would make it difficult to alter. When the system receives a message, it fetches the associated public key and authenticates the signature by recomputing the hash of the message. Where the check is a match, it is checked as verified, otherwise, not verified. Every effort irrespective of failure or success is kept in a different record to be traced. The mechanism will also ensure that the messages are not tampered with, identities of the sender can be determined, accountability upheld, and in the process, any message relayed by any source can be traced to its source without any doubt.

The Privex system is made to facilitate the accountability and non-repudiation of a secure communication. Pseudocode 2 describes the steps of this secure communication. It does it by signing every message digitally with the RSA privative key of the sender and validating the signature with the public key. This will ensure that all messages are easily traced into their source, thus eliminating the denial of the message being authored and enhancing trust among the involved parties. Also, the Pseudocode 2 enables auditability when meetings are held collaboratively. The same image (Figure 3) shows the message signing and verification process, which is a visual representation of the activity of the pseudocode 2.

Pseudocode 2 Non-Repudiation USING RSA Digital Signature

1. **START**
2. **CHECK** if password IS provided
3. **IF** password = NULL THEN
4. **RAISE** "Password required for key encryption"
5. **END IF**
6. **GENERATE** RSA key pair (2048 bits)
7. **ENCRYPT** private key using scrypt + AES-128-CBC with password
8. **SAVE** encrypted private key AS <username>_private.pem
9. **SAVE** public key AS <username>_public.pem
10. **LOAD** private key using password
11. **COMPUTE** SHA-256 hash of the input message
12. **SIGN** hash USING private key (PKCS#1 v1.5)
13. **CONVERT** signature **TO** hexadecimal
14. **LOG** (sessionId, username, signature, timestamp) **INTO** chat_logs.json
15. **RETURN** signature_hex
16. **LOAD** public key of sender
17. **COMPUTE** SHA-256 hash of received message
18. **CONVERT** received signature_hex TO bytes
19. **VERIFY** hash USING public key (PKCS#1 v1.5)
20. **IF** verification SUCCESS THEN
21. status ← "verified"
22. **ELSE**
23. status ← "not verified"
24. **END IF**
25. **LOG** (sessionId, username, status, timestamp) **INTO** chat_logs_verified.json
26. **RETURN** verification status
27. **END**

3.2.3 Dynamic Blocking System Algorithm

The dynamic block system facilitates access control in broadcasting, which is safe in real time. Dynamic because it can put a user instantly offline and create new encryption keys in real time - and leave other individuals offline. This ensures that the message is secret and trustful because the members who are not part of the group will never be aware of the future messages and the risk of an expelled member coming back is also not present due to the assistance of the older data. In its absence, this operation can be a security vulnerability, with breaches in reused tokens or the existing exchanges will be visible. The system works in accordance with the RSA to administer identity-related protection as well as the Diffie-Hellman (DH), which produces many symmetric keys of varying lengths. The first step is to create RSA sets by the session leader of that particular session; the remainder of the participants are then given the public part of the set.

In order to derive secure symmetric key, DH values (P and G) are generated - this allows every participant involved be it an organizer or an attendee to develop his or her own DH key, both the private and the public key. Both sides are swapped with public keys to come up with a shared secret. It is built on that shared output to build the encryption keys that are necessary on the session. In the case when the host has been banned, the site instantly removes the shared secrets according to the DH and erases all the information published previously, and breaks the current connections. When this happens, new DH values are obtained - which immediately renews the key of all the already-running members. This process and new secret pairs are created, and the material used in the old encryption will not be of any use to a deserted person. DH also offers forward secrecy to have an added bulk of security where any keys stored or sent will not be helpful when they are removed - making the connections of the connections safe and steady throughout the entire session.

To prevent the user privileges of a blocked user, the pseudocode 3 is created to implement real time access control and security of a session by revoking the privileges of the user immediately. On revocation, the algorithm causes the regeneration of Diffie-Hellman shared keys and voids all the previously utilized encryption content. This makes sure that participants that are removed cannot decrypt any further communication or resuming the session with the help of a cache. Pseudocode 3 makes forward secrecy strong and tightly couples the access control with the cryptographic protection during the entire lifecycle of the meeting by dynamically rekeying the session. This revocation and rekeying process is also shown in (Figure 4), and it is a graphical depiction of how the pseudocode 3 should work.

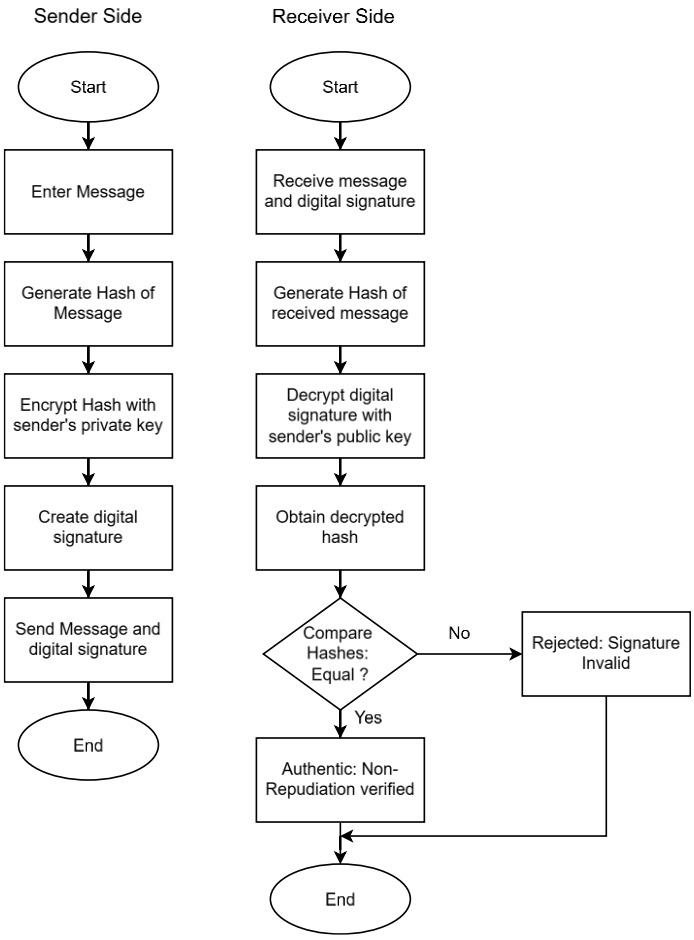


Fig. 3 Flowchart of Non-Repudiation

Pseudocode 3 Dynamic Blocking System

```
Initialize RSA Key Infrastructure
FUNCTION generate_meeting_keys_RSA(meetingID)
CREATE a pair of RSA public and private keys (2048 bits)
STORE keys as <meetingID>_public_key.pem and
<meetingID>_private_key.pem
END FUNCTION
FUNCTION RSA_Encrypt(public_key, message)
IMPORT public_key
ENCRYPT message using PKCS1_OAEP
RETURN base64 encoded ciphertext
END FUNCTION
```

```
FUNCTION RSA_Decrypt(private_key, ciphertext)
IMPORT private_key
DECRYPT ciphertext using PKCS1_OAEP
RETURN plaintext message
END FUNCTION
FUNCTION generate_dh_parameters(bits)
VALIDATE bits is multiple of 128 and > 512
q ← Generate large strong prime number of 'bits' length
g ← 2
RETURN (q, g)
END FUNCTION
CLASS DiffieHellman(p, g)
GENERATE private_key ← Random(2, p−1)
COMPUTE public_key ← g^private_key mod p
FUNCTION compute_shared_secret(received_public_key)
RETURN received_public_key^private_key mod p
END FUNCTION
END CLASS
FUNCTION generate_new_dh_key(username, meetingID, P, G)
host_dh ← DiffieHellman(P, G)
server_dh ← DiffieHellman(P, G)
host_secret ← host_dh.compute_shared_secret(server_dh.public_key)
server_secret ←
server_dh.compute_shared_secret(host_dh.public_key)
RETURN (host_secret, server_secret)
END FUNCTION
FUNCTION dynamic_block_user(blocked_user, meetingID)
MARK blocked_user.is_blocked ← True
FETCH updated active users list
//y Regenerate Diffie−Hellman shared keys for all remaining users
P, G ← generate_dh_parameters(1024)
FOR each user IN active_users DO
(user_key, server_key) ← generate_new_dh_key(user, meetingID, P, G)
UPDATE session_key(user, meetingID, user_key)
END FOR
DELETE blocked_user's old key pair FROM key database
NOTIFY all active users about session rekey event
END FUNCTION
IF host initiates blocking event THEN
CALL dynamic_block_user(blocked_user, meetingID)
REKEY all user sessions
END IF
End.
```

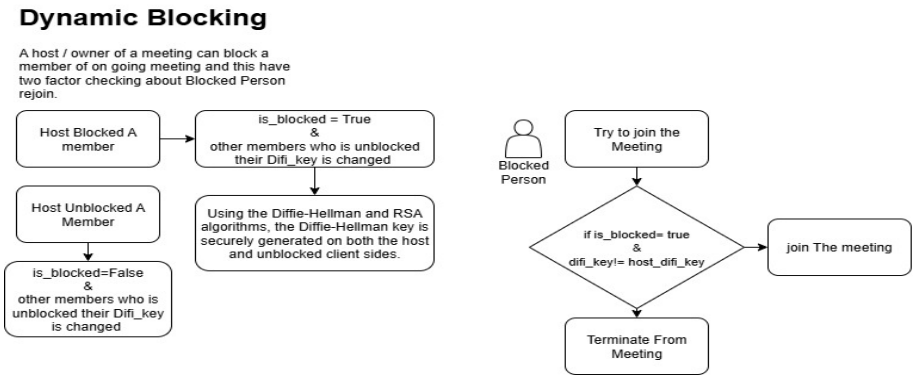


Fig. 4 Flowchart of Dynamic Blocking System

4 Resource & Technologies Used

4.1 Resources Used

The proposed system was developed and tested on the existing desktop and laptop systems that are capable of supporting the existing Python based web applications. It is supported on the Python 3.10 or later, and this choice is made as it is stable, has a comprehensive standard library, and may be combined with advanced cryptographic and networking libraries. Flask web framework is used as the back end that enables the use of secure sessions and RESTful development of services and Flask-socketIO is added to give real-time and two-way communications required during the live meeting, delivery of instant messages, dynamic blocking and co-host role administration. SQLite is a relational database that is based on user credentials, hashed passwords, session-data, encryption metadata, and access-control states since it is lightweight with low overhead and predictable transactional properties. Gunicorn is used to control deployment, where it is a WSGI-based server that is production-ready in order to have the requests processed effectively and scale to a number of users.

Cryptographic operations are done using a set of pre-established Python libraries. Cryptography library is implemented on AES-based symmetric encryption and Fernet and Multi-Fernet key management and safe end-to-end encryption processes. Cryptographic uses of the public key cryptography such as the RSA key generation, non-repudiation digital signature, and dynamic session rekeying using Diffie Hellman key exchange are done using the PyCryptodome (Cryptodomex). The hash of user passwords is computed using the hashlib provided with the built-in hashlib module implementing the SHA-256 hash and without storing the plaintext credential, and eliminating the risk of offline attacks. All of these technologies constitute a powerful, stable, and scalable platform that would facilitate the hybrid

cryptography protocols, real-time session management, and efficient access control in the communication platform suggested.

4.2 Technologies Used

The suggested cryptographic and session management framework required integration of a number of secure communication protocols and cryptographic mechanisms to provide confidentiality, integrity, authentication and non-repudiation. The architecture of the system is based on the hybrid encryption approach which is a combination of symmetric and asymmetric encryption methods. Advanced Encryption Standard (AES) [9] is used to obtain end-to-end encryption with individual user keys being safely concatenated with the principles of Multi-Fernet [10] based encryption to obtain a safeguarded session key. This session key is dynamically regenerated every time people join, leave, or are blocked, in order to have forward and backward secrecy all the time. Communication with partying entities through secure means is enforced with Transport Layer Security (TLS) [11] which avoids eavesdropping and tampering in message transfer. Strong authentication and accountability require that password-based authentication be carried out with the help of the cryptographic hash functions so that sensitive credentials are not stored or transferred in plaintext. Non-repudiation is carried out using RSA-based digital signatures [12] whereby each message is signed cryptographically by the sender and is checked by recipients through public-key checking. Password-based encryption is applied to the protection of the private keys which are only activated temporarily on authenticated sessions. The integrity of the session itself is further enhanced with the help of the signed authentication tokens and the message authentication codes to avoid the attacks of replay and impersonation. The reduction of verification latency is achieved with the use of public-key distribution and caching mechanisms. Together, these protocols and mechanisms constitute a resilient, secure and scalable communications framework that can be adapted to dynamic session changes and provide and sustain strong cryptographic guarantees.

5 Security Analysis

The proposed hybrid public key system will integrate a number of crypto-tools such as AES, Multi-Fernet [10] a symmetric encryption RSA signatures, as well as Diffie-Hellman, to provide a high-quality, full cover protection. In this case, we examine the system security level; simultaneously, investigate the resistance of the system to the common attacks.

5.1 Confidentiality

Security is also based on End-to-End Encryption [13] which is powered by AES [9]; in this case, the session key remains hidden by a multi-Fernet [10] configuration using user-specific AES codes. Intruders cannot decrypt messages unless they have all the necessary parts as the primary AES code is only created when the proper parts are combined. When a user enters, exits, or removes, the primary key is rebuilt with new pieces - the previous communications remain secure as well as the future communications are secured against easy surveillance by a simple spying - using the secure channels, no pieces of the data are leaked when transferring, and because the connections are encrypted by default, the systems cannot easily access the communication.

5.2 Integrity

The integrity of messages is ensured at two levels:

- AES Encryption Integrity: Fernet encryption relies on the HMAC [14] to test the integrity of data, and thus any manipulations with encrypted data can be noticed instantly.
- RSA Digital Signatures: Each message is signed with a digital signature of the secret key of a sender (secured through scrypt + AES-128-CBC). When a person changes it, RSA public-key verification indicates the change.
- Messages are stored in write-once formats, which prevent the ability to alter or forge messages in history. In combination, these two features make it impossible to alter or forge a message.

5.3 Authentication

- The system has various verification procedures with one being undertaken after another.
- Password hashing with SHA-256 will imply that even in case the database is compromised, the credentials are not retrievable.
- RSA private keys which are password protected enable only authorized individuals to use their decryption data by using secure authentication procedures.
- Due to the fact that messages require a personal key - and a key is unlocked upon your signing in - the origin remains validated.

5.4 Non-Repudiation

The RSA protocol ensures that every message can be successfully authenticated to the sender.

- Messages are instead signed using a private key.
- Check records which include working - and not working - are maintained in tamper-proof log files.

- A user is not able to deny that he/she sent a message later - this satisfies traceability requirements in legal situations.

5.5 Availability

The system provides availability by:

- Fast AES coding is ideal in real time data transfer since it maintains the speed of data transfer and also keeps security high.
- Rapid DH key renewal without breaking of active connections.
- Co-hosts replace the absent host and the sessions continue to operate without interruption. This removes any one point of failure while keeping meetings running smoothly.

5.6 Attack Categories

5.6.1 Attacker Type 1: Network Attacker (Dolev-Yao Adversary)

Definition: A Network Attacker A_{net}possesses full control over the communication channel, capable of intercepting, replaying, or injecting packets at will. The adversary has no valid credentials (id_X, pw_X) or session keys$K_{session}$.

Threat Analysis: The system is secure against A_{net} if the probability of breaking the end-to-end encryption (E2EE) is negligible:

$$Pr[A_{net}(C) \rightarrow M] \leq \epsilon(\lambda)$$

Where C is the intercepted ciphertext $E(M, K_{session})$. Because the master key K_{master} is derived via a multi-Fernet construct requiring n individual user keys:

$$K_{master} = MultiFernet(k_1, k_2, \dots, k_n)$$

An attacker without these keys cannot derive the plaintext. Furthermore, replayed ciphertexts are invalidated via session re-keying:

$$K_{session}^{(i)} \neq K_{session}^{(i+1)}$$

Where $\$i$ denotes the session state. Thus, A_{net} cannot recover key material or read session data.

5.6.2 Attacker Type 2: Malicious Participants

Definition: A Malicious Participant A_{int} is a legitimately authenticated user within session i. They possess a valid RSA key pair (PK_{int}, SK_{int}) and a specific AES key-share (k_{int})

Threat Analysis: To impersonate another user U_j , the adversary must forge a digital signatureσ_j:

$$\sigma_j = Sign\left(SK_j, H(M)\right)$$

The security of the system relies on the hardness of the RSA factoring problem. The probability of A_{int} successfully forging σ_j is:

$$Pr\left[A_{int}\left(PK_j, M\right) \rightarrow \sigma_j\right] \leq \epsilon(\lambda)$$

Additionally, since the session master key K_{master} requires all authorized shares, partial possession by A_{int} yields zero information:

$$H(k_{int}) \approx Uniform$$

All actions are bound by digital signatures stored in append-only audit logs, ensuring accountability.

5.6.3 Attacker Type 3: Removed User (Forward/Backward Secrecy)

Definition: A Removed User A_{rem} is an entity whose status has been updated to $is\_blocked = True$. They retain legacy key material $K_{session}^{(i-1)}$ from previous participation.

Threat Analysis: The Privex system enforces Perfect Forward Secrecy (PFS) and Backward Secrecy through dynamic re-keying. Upon a membership change, new Diffie-Hellman (DH) parameters are generated:

$$SS^{(i)} = g^{ab} \backslash pmodp$$

Where $SS^{(i)}$ is mathematically independent of $SS^{(i-1)}$. The probability of A_{rem} using stale material to decrypt future messages $C^{(i)}$ is:

$$Pr\left[A_{rem}\left(K_{session}^{(i-1)}, C^{(i)}\right) \rightarrow M^{(i)}\right] \leq \epsilon(\lambda)$$

The $is\_blocked$ flag acts as a non-cryptographic barrier that terminates the protocol before cryptographic processing even begins.

5.6.4 Attacker Type 4: Compromised Server Attack

Definition: This model assumes the adversary A_{srv}has gained administrative access to the server's database and memory.

Threat Analysis: Privex utilizes a Server-Assisted E2EE model. Sensitive data is never stored in plaintext:

- Passwords: Stored as $H(pw\_X)$ using SHA-256.
- Private Keys: Encrypted as $E(SK_X, scrypt(pw_X))$
- Session Keys: Encrypted via multi-Fernet; the server only acts as a relay for ciphertext C.

Even with full database access, the probability of A_{srv} recovering a private key without the user's password is:

$$Pr[A_{srv}(Encrypted\ SK_X) \rightarrow SK_X] \leq \epsilon(\lambda)$$

Because scrypt is a memory-hard function, brute-force attempts are computationally impractical.

5.6.5 Attacker Type 5: Network Eavesdropping

Definition: All end-to-end session messages are encrypted through end-to-end AES encryption, which means that any information intercepted will not be readable. The use of secure key exchange and signature verification between the Client and Server will prevent the compromise or forgery of the session key used in order to maintain the confidentiality of the messages sent between both Client and Server, as well as maintaining the integrity of the messages sent between both Client and Server from any network adversaries.

Threat Analysis: Read confidential session messages sent in the session; collect ciphertext transmitted in the session; deploy analysis to determine communication patterns; attempt to reconstruct plaintext from the captured data within the network.

Protection Mechanisms that are Mapped to this Threat:

- All messages sent within the session are encrypted end-to-end using AES via the Fernet encryption scheme before leaving the sending device.
- The communication channel is being secured using TLS, to provide encrypted communication between the Client and the Server.
- The Server does not process plaintext messages. The only message the Server/Client can process is ciphertext.

Even if an eavesdropper captures all packets traveling within a network, the communication that they intercepted is still going to be unreadable ciphertext (unless the eavesdropper is in possession of the session key). An eavesdropper who captures the communication transmitted will not gain any valuable information due to not having possession of the session key, therefor the eavesdropper will not have any useful data regardless of the number of packets they have captured.

5.6.6 Attacker Type 6: Man-in-the-Middle Attack

Definition: A man-in-the-middle (MITM) attack is when an attacker secretly intercepts and may also modify communications between two parties. An attacker can place themselves in between the sender and the receiver to listen to, modify, or insert into a communications session.

Threat Analysis: DENY: The attacker can intercept session messages; modify messages during transport; insert malicious messages into sessions; impersonate legitimate participants during sessions.

Protection mechanisms for this Threat:

- TLS-secured transport ensures no unauthorized interception of messages and confirms the authenticity of the connection.
- Each message includes an RSA-2048 digital signature that the recipient can verify to confirm the identity of the message's author.
- Diffie-Hellman key verification securely negotiates shared keys between participants.

A successful MITM cannot modify, insert, or impersonate a message without detection, in that all modifications to any message will cause the signature verification or the TLS validation to fail, and the message will be rejected by the recipient.

5.6.7 Attacker Type 7: Replay Attack

Definition: This is an attack where an attacker manipulates or falsifies data transmitted after it has been legitimately sent by the sender, to gain unauthorized access to something, or disrupt a service.

Threat Analysis: Capture existing ciphertext and re-use this ciphertext to re-play previously valid function calls, or messages and disrupt the integrity of a session by injecting messages into the existing session that are stale.

Protection Mechanisms Mapped to This Threat:

- Session AES keys are automatically rotated when any participant joins, leaves or has been blocked.
- Fernet encryption includes HMAC-SHA256 for integrity verification of each message ciphertext.

When the session key changes, old ciphertext becomes invalid and cannot be decrypted until the key has been changed, and therefore the captured data will also be deemed cryptographically stale immediately after key rotation. All previously replayed messages will fail HMAC validation and as a result will be rejected prior to their decryption.

5.6.8 Attacker Type 8: Message Forgery Attack

Definition: An attacker tries to impersonate a legitimate participant by fabricating and transmitting messages from the impersonated party to trick counterparts into believing they are receiving authentic messages.

Threat Analysis: Any messages can be fabricated using another's identity; there is an ability to inject unauthorized content into the conversation; an ability exists to manipulate the flow of a conversation.

Protection Mechanisms Mapped to This Threat:

- The RSA-2048 digital signature must be present in every message when generated by the original sender's private key.
- The signature generated on the messages uses SHA-256 Hashing algorithm with the PKCS#1 v1.5 Verification Method.
- Verification of all message signatures must take place prior to any messages being accepted.

An attacker cannot create a valid signature if access to the secret/private key belonging to the actual sender has not been granted. Furthermore, any forged message will never pass verification and will be rejected immediately.

5.6.9 Attacker Type 9: Message Tampering Attack

Definition: Unauthorized alteration of a legitimate message during transmission constitutes modification in violation of the integrity requirement with the intent of avoiding detection.
Threat Analysis: Change content of message; corrupt encrypted data; change meaning of the message by altering transmitted ciphertext.

Protection Mechanisms (Mapped to this Threat):

- Every encrypted message (using Fernet encryption) will use HMAC-SHA256 for authentication.
- Modification to the ciphertext will invalidate HMAC verification.
- The application layer uses a RSA digital signature to independently verify message integrity.

Detection of any modifications to the ciphertext occurs pre-decrypt. All tampered messages fail to verify integrity and will therefore be rejected by the system.

5.6.10 Attacker Type 10: Brute-Force and Cryptographic Resilience

The system employs high-entropy keys to prevent exhaustive search attacks:

- AES-128: Provides a key space of 2^{128}.
- RSA-2048: Relies on the integer factorization complexity.

$$Factoring\ N = p \cdot q\ where\ |N| = 2048\ bits$$

Computational infeasibility is maintained as long as $\lambda \geq 128$ for symmetric and $\lambda \geq 2048$ for asymmetric components.

5.6.11 Attacker Type 11: Private Key Theft Attack

Description: An attack against a user's private cryptographic key in order to gain access to the decryption of encrypted messages, or to create a digital signature that impersonates the user.

Threat Analysis: Stealing private keys to create false signatures and impersonate legitimate users' identities to gain unauthorized authorization for a message.

Defensive Mechanisms to Counter the Risk:

- RSA private keys will be encrypted with AES-128 CBC.
- The key to the private key will be generated using the scrypt password-based key derivation function.
- User passwords will not be stored in the system.

Utilizing a password related to a private key will render the private key useless. Attempting to perform a brute-force search for a password on a private key will take many years, due to the design of the memory-hard nature of the scrypt algorithm.

5.6.12 Attacker Type 12: Forward/Backward Secrecy Attack

Definition: This attack scenario includes forward secrecy failure when an adversary is capable of successfully decrypting previously sent messages after obtaining a compromise on a current (or prior) key and the backwards secrecy failure, where an adversary is capable of decrypting future messages based upon having obtained a compromise on the currently used key.

Threat analysis: This scenario allows an adversary to be able to use the current key to decrypt prior (or historical) messages; and also allows an adversary to be able to access a conversation history that was established prior to joining, as well as decrypting future messages after having left the session.

Protection Mechanisms that map to this Threat:

- Every time there is a change of participant membership, Diffie-Hellman re-keying generates a new and unique session key.
- The rotate_keys() mechanism generates new keys when any user joins or leaves the session.
- There is no mathematical relationship between the old keys and the new keys.

Even if the current key is compromised, past messages are protected and cannot be decrypted by new users that did not participate in the session prior to joining.

5.6.13 Attacker Type 13: Repudiation Attack

Definition: Defined as attempting to disavow / deny that you have done (action) or sent (message) while exploiting the fact that there is no verifiable proof mechanism available (i.e., evidence of the action has not occurred).

The following items fall under this category of threat:

Denying authorship of message(s) or avoiding responsibility for message(s) sent; questioning where messages came from (origin).

The following protection mechanisms have been mapped to this category of threat:

- All messages are digitally signed using RSA encryption/signature
- All digitally signed messages are maintained in Audit Logging in an Append Only Format
- Each record in the Audit Log contains the session id, the user name, the signature of the user that created the message, and date/timestamp

Having the sender's Public Key for a given message, allows you to verify authorship. The signed Audit Log records of messages provide a permanent, verifiable proof of who created the message.

5.6.14 Attacker Type 14: SQL Injection Attack

Definition: SQL injection attacks occur when input validation is performed improperly and allow an individual to insert malicious SQL statements into a SQL command, resulting in potentially obtaining access to, modifying or deleting data within a database (or data source).

Threat Analysis: This threat can extract confidential data from a database, modify stored information already within the database and bypass the authentication mechanisms employed by the database.

Protection Mechanisms That Mitigate This Threat

- All SQL statements that modify the database employ the use of parameterized queries through SQLite (i.e. Bound Variables).
- All input to a SQL statement is verified against strict input validation rules prior to the statement being processed.
- We have utilized a static analysis tool (i.e. Bandit) to identify and eliminate unsafe SQL statements from our application.

Therefore, SQL injection vulnerabilities will be addressed at the implementation level. As a result, there are no unauthorized database queries that can be executed by attackers.

5.7 Secure Implementation Validation and Static Code Analysis

In advance of the implementation of this proposed system, we performed a thorough static code analysis to verify the security integrity of the software. We used the Bandit (v1.8.6) tool to perform a pre-deployment scan on all the application's modules and on all dependencies in the virtual environment on August 19, 2025, with the total number of lines of code being 1,099,003. Once we found vulnerabilities in the scan, we fixed them, and after fixing the security vulnerabilities, we scanned the codebase again to verify that we had fixed the identified vulnerabilities. The results of the findings, the actions we took to fix the vulnerabilities, and the results from the re-scanning for remediation are all contained in this section, which serves as evidence that the system has performed all required security assessments to be in compliance.

CWE is a list of common software and hardware vulnerabilities that provides standardized definitions of the types of vulnerabilities that can exist as a result of a flaw in the design or implementation of the software, or the configuration of the device. CWE is maintained by the MITRE Corporation and is used as the basis for identifying and categorizing potential weaknesses in a system so they can be methodically assessed and remediated in the security assessment and validation process.

This research employs CWE to develop a framework for assessing the proposed architecture's ability to withstand attacks exploiting known categories of Software security weaknesses (e.g., misuse of cryptography, unauthorized access to the key management system, or flaws in authentication). The mapping of potential weaknesses and attack scenarios against relevant CWE categories helps validate that the proposed system was designed securely and mitigates exposure to known types of Software Security vulnerabilities. Therefore, using the CWE mapping strengthens the Security Analysis' credibility and aligns it with established Cyber Security Standards.

5.7.1 Initial Scan Results — Vulnerability Detection

The initial Bandit scan produced 80,542 flagged items across the codebase; after filtering results from third party packages in the virtual environment, there were found to be 59 vulnerabilities in the project's own source files across 15 modules; the details of the 6 vulnerability categories are summarized in Table 2.

Example Evidence — Detected Findings

The following examples reproduce representative Bandit output entries as direct evidence of the detected issues. Each entry shows the tool-reported issue identifier, severity rating, CWE reference, and the corresponding source location. Figure 5, Figure 6, and Figure 7 represent the output from the Bandit simulation run of the Privex.

Table 2 Vulnerabilities Detected During Initial Bandit Scan

Vulnerability	CWE	Severity	File(s) Affected	Issues
Deprecated pyCrypto-library	CWE-327	High	api.py, dh_rsa.py, rsa.py, non_repudiation.py	28
Flask debug=True in production	CWE-94	High	app.py	1
Hardcoded credentials	CWE-259	Low	app.py	2
XSS via Markup() rendering	CWE-79	Medium	app.py	1
SQL injection via f-strings	CWE-89	Medium	todo_db.py	3
Weak RNG for crypto keys	CWE-330	Low	dh_rsa.py, test.py	2

Example 1: Flask Debug Mode (app.py, line 841)

```
>> Issue: [B105:hardcoded_password_string] Possible hardcoded
   password: 'pbrp vfiq jijb gqwf'
      Severity: Low          Confidence: Medium
      CWE:                                          CWE-259
   (https://cwe.mitre.org/data/definitions/259.html)  Location:
   .\app.py:526
 525     sender_email = "privex.official.contact@gmail.com"
 526     app_password = "pbrp vfiq jijb gqwf"
```

Fig. 5 Bandit output — Flask debug mode vulnerability (pre-remediation)

Example 2: Hardcoded Password String (app.py, line 526)

```
>> Issue: [B201:flask_debug_true] A Flask app appears to be
   run with debug=True, which exposes the Werkzeug
   debugger and allows the execution of arbitrary code.
      Severity: High          Confidence: Medium
      CWE:                                        CWE-94
   (https://cwe.mitre.org/data/definitions/94.html) Location:
   .\app.py:841
  840    init_db()
  841    socketio.run(app, debug=True)
```

Fig. 6 Bandit output — Hardcoded credential vulnerability (pre-remediation)

Example 3: SQL Injection Vector (todo_db.py, line 148)

```
>> Issue: [B608:hardcoded_sql_expressions] Possible SQL
   injection vector through string-based query construction.
      Severity: Medium        Confidence: Medium
      CWE:                                        CWE-89
   (https://cwe.mitre.org/data/definitions/89.html)
   Location: .\todo_db.py:148
   • c = conn.cursor()
   • c.execute(f'"UPDATE Tasks SET {set_clause} WHERE id = ?'", values)
```

Fig. 7 Bandit output — SQL injection vulnerability (pre-remediation)

5.7.2 Remediation — Code-Level Fixes Applied

Each detected vulnerability was resolved through targeted code modification. The following examples (through Table 3, Table 4, and Table 5) illustrate the before-and-after state of the corrected code for three representative cases.

Fix 1: Disabling Flask Debug Mode

Table 3 Code fix — Flask debug mode controlled via environment variable

Before Remediation	After Remediation

# app.py — line 841 (before) 	
socketio.run(app, debug=True)
	# app.py — line 841 (after)
	debug_mode = os.environ.get('FLASK_DEBUG','false') =='true' socketio.run(app,debug= debug_mode)

Fix 2: Removing Hardcoded Credentials

Table 4 Code fix — Secrets migrated to environment variables.

Before Remediation	**After Remediation**

# app.py (before) 	
app.secret_key = 'hagkfgkew$#%^%$hag'
app_password = 'pbrp vfiq jijb gqwf'
	# app.py (after)
	app.secret_key = os.environ.get('SECRET_KEY')
	app_password = os.environ.get ('GMAIL_APP_PASS')

Fix 3: Parameterised SQL Query

Table 5 Code fix — Dynamic SQL column names validated against allowlist

Before Remediation	**After Remediation**

# todo_db.py (before) 	
c.execute(f'"UPDATE Tasks SET {set_clause} WHERE id = ?'", values)
	# todo_db.py (after)
	ALLOWED = {'title','status','priority'} if not set(cols).issubset(ALLOWED):
	raise ValueError('Invalid column') c.execute(query, values)

5.7.3 Post-Remediation Validation Results

Following the application of all fixes, the Bandit scan was re-executed under identical configuration. The post-remediation scan confirmed that all six vulnerability classes identified in the initial analysis were fully resolved. Table 6 presents a comparison of pre- and post-remediation issue counts per category.

Table 6 Pre- and Post-Remediation Issue Count Comparison

Vulnerability	Pre-Remediation	Post-Remediation	Status
Deprecated pyCrypto library	28	0	Resolved
Flask debug=True in production	1	0	Resolved

Hardcoded credentials	2	0	Resolved
XSS via Markup() rendering	1	0	Resolved
SQL injection via f-strings	3	0	Resolved
Weak RNG for crypto keys	2	0	Resolved
TOTAL (source files)	37	0	Resolved

The validation process has been demonstrated in Table 6, which represents a complete security lifecycle, including automated detection, targeted remediation, and verified resolution, confirming that the system has zero security vulnerabilities as identified during initial security assessment and that it passes the security validation criteria for a production deployment. The validation results also support the integrity claims of the system as documented in this paper.

In Table 7, The security characteristics and cryptographic methods within Privex can be found in the Privex framework. Privex implements confidentiality at the highest level by encrypting data from end to end using AES encryption and subsequently encrypting the data using the Fernet encryption model. Because of this, only those who are intended recipients of the information will be able to decrypt the sent information, and thus, all other parties will not have access to the same information. In addition to confidentiality, Privex uses the HMAC and RSA signature algorithm to ensure the integrity of sent information; therefore, if any changes or tampering were made to send information at any point, the user would instantly know. To provide authentication, Privex uses a password hashing mechanism based on the SHA-256 hashing algorithm. Therefore, only registered users will have access to the cryptographic resources. Lastly, to provide non-repudiation, Privex offers a mechanism for creating a link between actions taken by users and the users themselves by using RSA digital signatures along with append-only audit logs. Therefore, the audit logs will link actions to an individual user, making it impossible for a user to deny an action taken.

6 Result

The length of time required to encrypt and decrypt each record, to rekey, and, also, compute the block response time is achieved through the use of Python's time module by recording a time stamp immediately before and after executing a test using time(). The delta (difference) between the ending time and beginning time is equal to the total execution duration in seconds. Additionally, by placing timing statements in the user simulation function, individual users' session times may be measured as well. Using this method

allows the accurate evaluation of the system's level of performance, response time, and scalability when subjected to concurrent user load.

Integrated Cryptographic & Session Memory Unit: The system requires an AMD Ryzen 5 5500U with Radeon Graphics paired with 16GB RAM to provide the computational multi-threading and memory capacity necessary to execute hybrid RSA-2048 and Diffie-Hellman operations while simultaneously managing the memory-hard scrypt algorithm for private key protection ; this specific hardware setup ensures the device can maintain stable encryption times (42.36 ms to 74.42 ms) and handle the significant rekey latency (up to 2864.89 ms) and blocking response times (up to 3778.4 ms) required for secure real-time sessions with up to 250 participants.

Table 8 presents the performance metrics of the proposed system under varying numbers of participants (10, 100, and 250). As the participant count increases, the rekey latency rises significantly from 209.20 ms to 2864.89 ms, indicating higher overhead during key updates in larger groups. Encryption time remains relatively stable, ranging between 42.36 ms and 61.58 ms, while decryption time shows a gradual increase from 2.05 ms to 8.3 ms. The blocking response time also increases with scale, from 3236.75 ms to 3778.4 ms, reflecting the additional processing and coordination required as the group size grows.

Table 7 Security Analysis table

Security Property	Mechanism Used in Privex	Effectiveness
Confidentiality	AES-based End-to-End Encryption with Multi-Fernet	Messages are encrypted at the sender and decrypted only by legitimate recipients. The server never accesses plaintext data, ensuring true end-to-end confidentiality.
Integrity	HMAC (via Fernet) + RSA Digital Signatures	Any modification of encrypted data is immediately detected. Digital signatures prevent message forgery or tampering.
Authentication	SHA-256 Password Hashing + Password-Protected RSA Private Keys	Ensures only authenticated users can access cryptographic keys and participate in communication.
Non-Repudiation	RSA Digital Signatures with Append-Only Audit Logs	Cryptographically binds messages to senders and prevents denial of message authorship.
Forward Secrecy	Diffie–Hellman Key Exchange with Rekeying	Past communications remain secure even if current keys are compromised.

Backward Secrecy	Key Regeneration on User Join/Leave/Block	New participants cannot decrypt previously exchanged messages.
Dynamic Access Control	Diffie–Hellman-Based Dynamic Blocking System	Immediately revokes access and invalidates keys of blocked users in real time.
Replay Attack Resistance	Session-Specific Keys with Automatic Rotation	Previously captured messages cannot be replayed after key updates.
Man-in-the-Middle Protection	RSA Authentication + Diffie–Hellman + TLS	Prevents interception, impersonation, and manipulation during key exchange and communication.
Key Leakage Protection	Encrypted Private Keys + Multi-Fernet-Based Key Distribution	Prevents exposure of complete session keys even if partial data is compromised.
02Insider Attack Mitigation	Digital Signatures and Per-User Key Shares	Legitimate users cannot impersonate others or access unauthorized session data.
Availability	Lightweight Cryptography and Co-Host Delegation	Ensures uninterrupted communication and eliminates single points of failure.

Table 8 Performance Metrics Across Varying Numbers of Participants

Number of Participants	Rekey Latency (ms)	Encryption Time (ms)	Decryption Time (ms)	Blocking Response Time (ms)
10	209.20	42.36	2.05	3236.75
100	1385.69	55.1	4.1	3556.68
250	2864.89	61.58	8.3	3778.4

The graphs in Figure 8 show that as the number of participants increases, rekey latency, decryption time, and blocking response time also increase due to higher system workload. In contrast, encryption time remains relatively stable with only minor variation. This indicates that the encryption process scales efficiently compared to other operations.

Table 9 shows the comparative performance analysis of Privex with the relates schemes with respect to the cryptographic primitive usage, architecture, etc. In comparing the features of the Privex proposed system with existing RSA-only and AES-only secure chat systems, previously published works like Singh et al. [15], as well as Singh et al. [16], are based solely on the AES symmetric encryption algorithm; while this algorithm performs well with encrypting messages, it does not provide adequate

strength in either key distribution or authentication methods to be considered a viable option. In comparison to those two studies, other systems like Carranza et al. [17] and Sönmez and Abbas [18] rely on a mix of both RSA and AES to provide both secure transmission of keys for authenticity and provide significant amounts of additional processing power for the secure transmission of both the keys for authenticity and the messages themselves.

Like the previous examples, Perkasa et al. [19], utilize Diffie Hellman along with AES, however they focus primarily on how they implement Diffie Hellman as a method of increasing the micro-service scalability as opposed to managing the dynamics associated with how to maintain the topography of a larger service. The Privex architecture, utilizing AES encryption, RSA digital signatures, and the Diffie-Hellman key exchange methodology, effectively creates a hybrid security model to optimally provide a high level of cryptographic security.

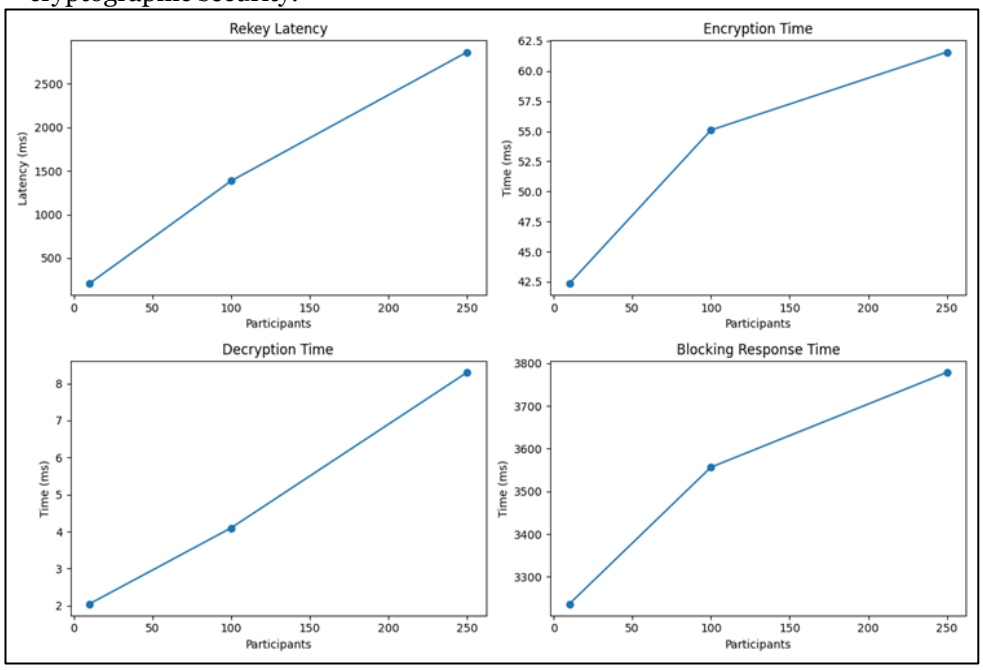


Fig. 8 Performance Analysis of Rekeying, Encryption, Decryption, and Blocking Operations with Increasing Participants.

AES quickly encrypts messages from one end to another while also providing the ability to authenticate, confirm that the private key is secure, and ensure non-repudiation using RSA. Diffie–Hellman provides an efficient way to create a new session key dynamically during an event (e.g. join/leave/blocking) so that a new session is always being created. This ensures both forward and backward secrecy. The proposed system is based on Python Flask (back-end), Flask-SocketIO (real-time client-server

communication), SQLite (session management), and allows for real-time efficient communication with secure key management.

In addition, Privex model is proven by the comparison charts to be more efficient operationally than the single algorithm method due to its application of only one algorithm to encrypt messages and signing (via RSA), and exchanging keys (via Diffie-Hellman) as well as less computation time than RSA only based systems while maintaining a greater level of assurance that the sender and receiver are who they claim to be compared to AES only based systems.

Finally, the dynamic re-keying and blocking functions supporting secure group communication do not significantly affect encryption/decryption performance. The performance charts and comparison table show that the Privex architecture will have significantly improved scalability, greater assurance of both security and performance than any currently available products.

Table 9 Comparison based on AES & RSA Efficiency, Key Exchange, and System Architecture.

Attribute	Singh et al. (2023) AES Android Chat [15]	Carranza et al. (2024) E2E Secure Chat [17]	Perkasa et al. (2025) DH+AES-256 Micro service [19]	Singh, Utama & Fat (2023) AES Chat Simulator [16]	Sönmez & Abbas (2017) RSA Client/ Server [18]	Privex
AES Usage	AES-128 for SMS & text message encryption	AES (CBC mode) for message encryption; session-specific keys.	AES-256 CBC for all message encryption	AES-256 in CBC mode for all chat messages	Not used; RSA-only system	AES via MultiFernet for E2E session encryption
RSA Usage	Not used (symmetric-only approach)	RSA for key exchange and key pair generation	RSA for digital signatures; key exchange via DH	Not used; symmetric-only system	RSA for both layers: client-server and client-client	RSA-2048 for digital signatures, non-repudiation, and private key protection
Key Exchange	Shared private key pre-established in app	RSA public key exchange then AES session key	Diffie-Hellman key exchange for shared secret	DH suggested for key exchange (future scope only)	RSA public key distribution between clients and server	Diffie-Hellman for dynamic session key exchange and blocking

Architecture	Android + SQLite; client-server	Python + tkinter GUI; client-server with sockets	Microservice: Nginx, WebSocket, Chat Service, RabbitMQ, PostgreSQL	Python CLI simulator; peer-to-peer via sockets	Client/server in MATLAB; two-layer RSA architecture	Python Flask + Flask SocketIO +SQLite; modular session-management backend
Order / Mode	Symmetric only; CBC mode implied	RSA (key exchange) then AES (message encryption); dual-layer	DH key exchange then AES-256 CBC encryption; scalable pipeline	Symmetric only; CBC mode for replay/MITM protection	Two-layer RSA: Layer 1 clients-server, Layer 2 clients-chat room	AES (E2E)+RSA (signatures) + DH (dynamic blocking); auto-rekeying on join/leave/block
Efficiency	Moderate - suitable for SMS-based mobile use; no asymmetric overhead	High - RSA adds overhead at setup but AES ensures fast real-time messaging	Very High - low latency, high throughput; benchmarked across 10-100,000 messages	Moderate - fast symmetric encryption; key sharing is main vulnerability	Low-Moderate - RSA-only is computationally expensive; small-scale use only	High - forward & backward secrecy; dynamic blocking; validated with Bandit static analysis

7 Conclusion

The proposed secure communication system combines various encryption systems to create an effective but simple communication tool. When employing AES, it employs the Multi-Fernet Encryption, to provide an end-to-end security system, keeping the data confidential and the keys in a safe location. Rather than using the symmetrical encryption only, it incorporates the RSA powered digital signatures to ensure that users can check the source of messages and avoid being denied of participation. Moreover, a Diffie-Hellman-based session control approach enhances user security since it allows administrators to block users, within no time, without disruption of ongoing chats. The Co-Host Delegation role enhances collaboration since it enables the transfer of control to be flawless throughout the meeting process, but it is extremely protective. It is tested and shows that the setup maintains high safety and at the same time does not compromise the convenience, fastness, or the desire to expand - which is perfect in virtual meetings, business correspondence, or collaborative work environments.

8 Future Scope

The proposed design may develop to meet the requirements of new trends in safety and convenience. Rather than the existing practices, the inclusion of

blockchain could be beneficial to store the session record and encryption evidence. Such a solution would result in an impeccable history that is more transparent. The other course of action would be to implement quantum resistant cryptography that would protect against the threats of powerful computers of the future. By adding AI-based anomaly detection, one can enhance the safety efforts by detecting bizarre activities - e.g., an unauthorized log-in or an internal risk - in real-time. To expand coverage, it might be relevant to address the system to different environments, such as mobile-native applications and minimal client installations, to expand usage by providing easier access. Speed maximization is important, especially when high-volume operations are involved, and smart key sharing and high-quality encryption reduce lag. Permission frameworks are better than broad rules because with permission frameworks it is much easier to control who can do what, usually by role or specific trait. Additionally, by combining encrypted cloud archives with zero-knowledge verification, it is possible to store the messages and documents safely over a long period of time, which suits the needs of larger organizations better.

Acknowledgment

We would like to take this opportunity to thank everyone who has helped to make this research project possible. We sincerely appreciate our supervisor and professor Dr Sudip Kumar Palit who has provided thorough and constant support through encouragement and provided great ideas and constructive feedback during our time together; his expertise has been essential to the success of this project as well as the decision on how the project would progress, the information required to complete the project and finally the conclusion of the project.

We would like to also thank our Institution UEM, Kolkata for providing the required materials, resources and support needed to complete this study. To Every author and peers, we appreciate the help in supporting through the collaboration, discussions and suggestions provided over our period of work together. We sincerely thank you all for the wonderful results of your effort and support through our time together.

Contribution of Each Author

Conception: Tiyasa Paul, Rohan Samanta, Pratik Saha, Partha Pratim Chaulia, Sudip Kumar Palit, Design of the work: Pratik Saha, Rohan Samanta, Investigation: Tiyasa Paul, Rohan Samanta, Data analysis and interpretation: Pratik Saha, Partha Pratim Chaulia, Drafting the article: Tiyasa Paul ,Partha Pratim Chaulia, Review editing of the article: Sudip Kumar Palit, Tiyasa Paul, Pratik Saha, Critical revision of the article: Sudip Kumar Palit, Final approval of the version to be published: Sudip Kumar Palit.

Conflict of Interest Statement

The authors declare no conflict of interests.

References

1. M. A. Jerlin, R. Shrivastav, K. Anusha, G. G. Devarajan, and S. M. Nagarajan, "Secure chat system: Harnessing the power of hybrid encryption for enhanced security and confidentiality," in *Proc. Int. Conf. Recent Trends Comput.*, Singapore: Springer, Jul. 2024, pp. 109–124.
2. M. A. Almaiah, Z. Dawahdeh, O. Almomani, A. Alsaaidah, A. Al-Khasawneh, and S. Khawatreh, "A new hybrid text encryption approach over mobile ad hoc network," *Int. J. Electr. Comput. Eng.*, vol. 10, no. 6, pp. 6461–6471, 2020.
3. Y. Fouzar, A. Lakhssassi, and M. Ramakrishna, "A novel hybrid multikey cryptography technique for video communication," *IEEE Access*, vol. 11, pp. 15693–15700, 2023.
4. L. Harn and C.-F. Hsu, "A practical hybrid group key establishment for secure group communications," *Comput. J.*, vol. 60, no. 11, pp. 1582–1589, 2017.
5. S. Ahmad, S. Mehfuz, and J. Beg, "Hybrid cryptographic approach to enhance the mode of key management system in cloud environment," *J. Supercomput.*, vol. 79, no. 7, 2023.
6. J. Sivakumar and S. Ganapathy, "An effective data security mechanism for secured data communications using hybrid cryptographic technique and quantum key distribution," *Wireless Pers. Commun.*, vol. 133, no. 3, pp. 1373–1396, 2023.
7. M. A. Jerlin, R. Shrivastav, K. Anusha, G. G. Devarajan, and S. M. Nagarajan, "Secure chat system: Harnessing the power of hybrid encryption for enhanced security and confidentiality," in *Proc. Int. Conf. Recent Trends Comput.*, Singapore: Springer, Jul. 2024, pp. 109–124.
8. K. Bhatele, A. Sinhal, and M. Pathak, "A performance-centric comparative study of hybrid security protocol architectures," in *Proc. AISOBE 2012*, India: Springer, 2012.
9. A. M. Abdullah, "Advanced encryption standard (AES) algorithm to encrypt and decrypt data," *Cryptography and Network Security*, vol. 16, no. 1, p. 11, 2017.
10. D. K. Zala and M. A. Khan, "Compressive method for securing text data using Base64 encoding and Fernet cryptography," in *Proc. 2nd Int. Conf. Sustainable Comput. Smart Syst. (ICSCSS)*, IEEE, 2024.
11. R. Oppliger, *SSL and TLS: Theory and Practice*. Norwood, MA, USA: Artech House, 2023.
12. J. H. Seo, "Efficient digital signatures from RSA without random oracles," *Inf. Sci.*, vol. 512, pp. 471–480, 2020.
13. F. Affan and R. Rehan, "Secure chat application end-to-end encryption," *The Multidisciplinary Edge: Advancing Academic Research & Development*, p. 138, 2025.

14. D. L. Hoang and T. L. Tran, “New proofs for pseudorandomness of HMAC-based key derivation functions (RFC 5869),” *J. Inf. Secur. Appl.*, vol. 93, p. 104179, 2025.
15. S. Singh, H. S. Utama, and J. Fat, “Chat simulator using AES encryption,” *Int. J. Appl. Sci. Technol. Eng.*, vol. 1, no. 3, pp. 931–940, 2023.
16. V. Singh, S. Janarthanan, U. K. Roshan, and N. Vaid, “A secure web-based Android chat application using the AES encryption algorithm,” in Proc. 2023 5th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)., Dec. 2023.
17. H. Carranza, M. Bustamante, A. Carranza, and S. Muniganti, “Secure chat application with an end-to-end encryption.” In *Proceedings of the World Congress on Electrical Engineering and Computer Systems and Science*. Avestia Publishing. doi:10.11159/cist24.140.
18. F. Sönmez and M. K. Abbas, “Development of a client/server cryptography-based secure messaging system using RSA algorithm,” *J. Manag. Eng. Inf. Technol.*, vol. 4, no. 6, 2017.
19. M. J. P. Perkasa, H. M. Ramdan, A. J. Maliki, and Somantri, “Implementation of secure end-to-end encrypted chat application using Diffie–Hellman key exchange and AES-256 in a microservice architecture,” *Eng. Proc.*, vol. 107, no. 1, p. 98, 2025.

Tiyasa Paul is a final-year B. Tech student in Computer Science and Engineering, specializing in Artificial Intelligence and Machine Learning at University of Engineering and Management Kolkata, India. Her undergraduate studies began with completing Secondary and Higher Secondary Education at Maria's Day School, Howrah. She has done work related to artificial intelligence and possess a strong interest of research in this field of study.

Rohan Samanta is a final-year B. Tech student in Computer Science and Engineering, specializing in Artificial Intelligence and Machine Learning at University of Engineering and Management Kolkata, India. He attended Lakshya High School throughout his education history and has a profound interest in emerging technology and software development careers.

Pratik Saha is a final-year B. Tech student in Computer Science and Engineering, specializing in Artificial Intelligence and Machine Learning at University of Engineering and Management Kolkata, India. He went to Bidhannagar Government High School for all of his schooling history, and is seeking to create practical applications that utilise both artificial intelligence and machine learning technologies.

Partha Pratim Chaulia is a final-year B. Tech student in Computer Science and Engineering, specializing in Artificial Intelligence and Machine Learning at University of engineering and Management Kolkata, India. He completed his school education in Secondary Education at Ramakrishna Mission Vidyabhavan and completed his study for Higher Secondary Education at Jafala Adarsh Vidyayatan; and has an interest in Intelligent Systems and creating innovative solutions.

Sudip Kumar Palit is an Associate Professor and Centre-in-Charge of the Cybersecurity Centre of Excellence at the University of Engineering and Management (UEM), Kolkata. He received his Ph.D. in Computer Science and Engineering from UEM in 2025. With 15 years of teaching and 10 years of research experience, his research interests include cybersecurity, cryptography, blockchain, SOC-SIEM frameworks, performance analysis of blockchain systems, and authentication protocols. He actively mentors' students in applied cybersecurity research and development.

The inaugural issue of the *Interdisciplinary Journal of Computing & AI (IJCAI)* establishes a rigorous and forward-looking platform for high-quality research at the intersection of computing and artificial intelligence. Featuring contributions from institutions across the United States, Sweden, and India, this issue reflects the global relevance of emerging technologies.

With a selective acceptance rate of 35% and all papers indexed in OpenAIRE, the journal emphasizes quality, transparency, and international visibility. The research spans key domains including healthcare analytics, AI systems, blockchain-enabled learning, cyber-physical security, and privacy-preserving technologies.

IJCAI invites researchers and practitioners to be part of this evolving interdisciplinary research community.

Aspiration Publishing Trust, 150, Motijheel Avenue, Dum Dum, Kolkata 700074, WB, India