Exploring the Role of Explainable AI in Attack Modeling for IoT Networks

Discipline: Computer Science

Blessy Thomas

Abstract - In an era marked by the pervasive presence of Internet of Things (IoT) networks, it is critical to ensure the strong security of these autonomous systems. The integrity, confidentiality, and availability of IoT networks are threatened by new, complex security concerns that have arisen as a result of the rapid expansion of these networks. Vulnerabilities in the IoT are often exploited by the attacker to gain unauthorized access endangering privacy and security of the network. Identifying potential attack paths in the connected ecosystem is essential for implementing strong security measures. With attack modeling, security experts can evaluate the potential attack paths in the network. We propose a new framework for attack modeling in IoT networks by incorporating Explainable AI(XAI). The XAI algorithm LIME (Local Interpretable Model Agnostic Explanations) has been included in the proposed framework to enhance the explanation and comprehension of the critical attack paths predicted. A use case is discussed and various graphs with explanations are provided to evaluate the performance of the attack model against the evolving dynamics of the IoT network. XAI provides a crucial layer of defense for protecting IoT networks from cyber hazards by offering interpretable insights into strong security decisions.

Index Terms **-** Machine Learning, Deep Learning, Explainable AI, IoT Network Security, Vulnerability Analysis, Attack Mod- elling.

I. INTRODUCTION

The Internet of Things (IoT) unifies billions of intelligent objects that connect with little to no human involvement [1]. Smart bulbs, cameras, televisions, and competent vacuum cleaners are a few of the everyday IoT devices that are linked to home and enterprise networks. This leads the network to become an easy target for attackers, who can readily hide their fraudulent actions among the amounts of data [2]. Most organizations have made significant investments to protect their data and networks from external and internal threats, by implementing sophisticated strategies [3]. The dynamic and quickly changing nature of these attacks makes it difficult for traditional cybersecurity techniques to keep up. The potential attack surface for attackers grows tremendously as IoT devices become an essential component of our residences, workplaces, factories, and even vital infrastructure. The risks are wide- ranging and constantly changing, ranging from unauthorized access and data breaches to device manipulation and Denial- of-Service (DoS) attacks. Therefore it is ineffective to implement security measures such as encryption, authentication, access control, network security, and application security for IoT devices and their underlying vulnerabilities. To effectively safeguard the IoT ecosystem, it is crucial to enhance existing security techniques. This is where the power of Machine Learning (ML) and Deep Learning (DL) come into play, heralding a paradigm shift in how we perceive security research within IoT networks.

Attackers often use the easiest paths to get inside the network. After identifying and prioritizing the vulnerabilities, it is important to model the attacker's pathways in advance to prevent all the possibilities of an attack [4]. Graphs can effectively illustrate vulnerability relations in a network since they are good at depicting relationships between elements [5]. The use of graphs in attack modeling has prevailed for the last several decades. Several graphical representations, such as attack graphs [6], attack trees [7], and attack-defense trees [8], are in use. Among these attack models, attack graphs are most widely used in representing vulnerability relations. The attack graph can show the attacker's paths to reach the desired system state [6]. DL and ML can assist with the automatic generation of attack graphs based on system parameters and recognized vulnerabilities promise to transform the cyber security environment.

Although ML and DL models excel, it can be difficult for human operators to trust and comprehend their judgments because of the intricate and opaque inner workings. XAI serves as a link between cutting-edge AI methods and human cog- nition. XAI promotes trust and accountability in IoT security by offering visible and comprehensible justifications for the decisions made by ML and DL models.

The concept of XAI gained prominence in the early 21st century as researchers and practitioners recognized the importance of developing AI models and techniques that could provide un- derstandable and transparent explanations for their decisions.

Since then, XAI has evolved rapidly, with various methods and frameworks designed to enhance the interpretability of AI systems, making them accountable, ethical, and applicable in domains where human comprehension is critical. With a large number of networked devices, protocols, and configurations, IoT ecosystems can be extremely complex. Without adequate justifications, it might be difficult to comprehend the risks and vulnerabilities in such environments. To provide interpretable insights into the vulnerabilities found and their possible effects, XAI can simplify the complexity of interpreting traditional attack modeling.

Local Interpretable Model-Agnostic Explanations (LIME), a potent XAI algorithm, holds significant importance in improving the clarity and interpretability of complicated machine learning and deep learning models [30]. Incorporating this XAI algorithm in attack modeling enables organizations to make wise choices on countermeasures, strengthen their security posture, and successfully address vulnerabilities in their IoT networks.

The rest of the paper is organized as follows, in section II we discuss the related works which include the role of ML and DL in IoT security, the importance of XAI in IoT network security, and attack modeling. In section III we explore the role of XAI in attack modeling and address the dynamic features of IoT. The proposed framework is explained in section IV and section V discusses the case study we conducted. The conclusion and future works are presented in section V.

II. RELATED WORKS

In this section, we discuss the prominent works in IoT network security that use ML and DL. Further, we discuss the importance of XAI in securing IoT networks and the existing attack modeling techniques.

a. ML and DL for IoT network security

IoT vulnerability assessment locates and resolves security flaws or vulnerabilities inside IoT ecosystems. It includes the identification and prevention of potential attack vectors that might take advantage of these weaknesses. Traditional attack detection and mitigation strategies rely on cryptographic primitives, which can occasionally be inaccurate and result in false positives, which demands the need of ML-based methods. The proposed method in [9], MANDRAKE, aims to detect vulnerabilities in IoT network traffic by analyzing packet traffic using machine learning techniques. This analysis helps identify potential vulnerabilities in traffic encryption, which is essential for ensuring the security of IoT networks. Similarly, LNKDSEA, a hybrid ensemble algorithm that ef- ficiently identifies various types of attacks in IoT networks, including DDoS, information gathering, malware, injection attacks, and man-in-the-middle attacks is introduced in [10] LNKDSEA combines Logistic regression, Na¨ÿve Bayes, K- nearest-neighbour, Decision tree, and Support Vector Machine to achieve high performance in detecting cyberattacks in both binary and multi-class classifications. The authors in [11] propose a solution for detecting and classifying attacks on IoT networks using novel ensemble techniques, CatBoost and XGBoost, trained on the realistic Edge-IIoTset Dataset. A distributed attack detection technique for IoT utilizing a deep learning approach was suggested in [12]. By employing deep learning techniques, the strategy seeks to identify assaults in IoT networks. Twenty Raspberry Pi IoT devices that had been infected were used by the authors in their studies, and they were successful in detecting attacks with an accuracy of 96 percent. The authors in [13] discuss the challenges of cybersecurity in IoT and propose a novel distributed deep learning scheme for cyber-attack detection in fog- to-things computing. The proposed approach concentrated on fog-to- thing communication and implemented the learning module at the fog layer, which is the best place for a detection mechanism because it both decreases communication latency and makes use of the available resources. The accuracy of the proposed three-layer stacked autoencoder is 99.2 percent. Hybrid deep learning models, which combine different deep learning techniques, are gaining attention for improving the detection of cyber-attacks in IoT networks. The authors in [14] propose a hybrid deep learning model using CNN and LSTM for detecting attacks in IoT devices with an accuracy of 96 percent.

b. Explainable AI for IoT network

In IoT networks with critical application infrastructures to foster trust, it is crucial to comprehend how AI-based security systems make judgments. In high-risk circumstances, transparency is crucial, and XAI offers it by outlining the rationale behind and process of each security decision and action. In [15] authors apply XAI to generate explanations for incorrect classifications made by data-driven Intrusion Detection Systems (IDSs). An adversarial approach is used to find the minimum modifications required to correctly classify misclassified samples, and the magnitude of these modifications is used to visualize the most relevant features that explain the reason for the misclassification. XAI is used in the context of secure Cloud-Edge deployments to provide explainable assessments of the security level of IoT applications in [16]. The methodology presented in the paper allows for automatically obtaining an explainable assessment of the security level of possible application deployments. XAI helps in expressing security requirements for IoT applications and infrastructure security capabilities in a simple and declarative manner. The authors in [17] advocate for the integration of domain knowledge into XAI models. By incorporating domain-specific expertise, XAI-enhanced IDR systems aim to provide more transparent and interpretable intrusion detection outcomes, thus enabling security analysts to better understand the rationale behind security alerts and facilitate more effective response strategies. In [18] authors introduce an innovative framework that combines deep learning techniques with ex- plainability mechanisms. This framework not only provides effective intrusion detection but also offers transparent and interpretable results, allowing security professionals to under- stand the rationale behind detected intrusions. By leveraging the power of deep learning while ensuring explainability, this research contributes to the advancement of IoT security, addressing the growing need for robust and understandable intrusion detection systems in IoT ecosystems.

Security experts can benefit from using XAI to better under- stand the types of vulnerabilities and attacks that can occur in IoT networks. It offers insights into the attack patterns and provides justifications for security alerts. XAI assists in adjusting security measures by outlining the dangers and vulnerabilities particular to each IoT environment.

C. Attack modelling

In attack modeling, attack graphs are important for locating and visualizing probable attack paths that an attacker could use to breach a system. Security experts can better understand the security posture of their systems and spot possible vulnerabilities that can be fixed to increase overall security by analyzing attack graphs. In [19] the authors introduced the idea of attack graphs and suggested an automated process for creating and analyzing them, which is a significant contribution to cybersecurity. The methodology consists of three basic steps: modeling the network, modeling the abilities and goals of the attacker, and creating the attack graph. The authors use formal methods, such as model checking, to verify the correctness of the generated attack graph.

The automatic generation and analysis of attack graphs is now necessary for defending IoT systems. Automated generation and analysis of attack graphs make use of machine learning and deep learning techniques to find emerging dangers and weaknesses in the IoT ecosystem. Machine learning and deep learning techniques enable real-time monitoring, rapid threat response, and proactive defense, making the automatic generation and analysis of attack graphs indispensable for safeguarding IoT systems against cyberattacks. The authors in [20] propose a methodology for building attack circuits that uses input/output pairs created by Natural Language Process- ing (NLP). The weights are also calculated using conventional security score metrics, and attack circuits are assessed using effective optimization methods. The contribution consists of a methodology that analyses possible attack vectors depending on their impact, exploitability, or overall risk. The authors use Fuzzy Petri Net (FPN) to establish an attack model and improve Q- Learning through FPN in [21]. They define the attack gain from the attacker's perspective to determine the best attack path. The paper introduces a quantitative indicator for analyzing the impact of cyber attacks on the real-time operation of power grids. The contribution is an attack model that enhances a Q-Learning algorithm with the use of FPN's fuzzy reasoning capabilities and further uses the Q-Learning algorithm to identify the network system's vulnerable part. An Autonomous Security Analysis and Penetration testing framework (ASAP) that uses attack graphs to identify security threats and attack paths in a network is introduced in [22]. The framework incorporates a state-of-the-art reinforcement learning algorithm based on Deep-Q Network (DQN) to determine the optimal policy for performing penetration testing. It also includes a domain-specific transition matrix and reward modeling to capture the importance of security vulnerabilities and the difficulty in exploiting them. The ASAP framework generates autonomous attack plans and validates them against real-world networks, making it applicable to complex enterprise networks. The attack involves injecting a predefined subgraph into a testing graph, causing the GNN classifier to predict an attacker-chosen target label for that graph. The attack is shown to be effective with minimal impact on the GNN's prediction accuracy for clean testing graphs.

In dynamic IoT networks, attack modeling is an ongoing process that changes as the network changes. It helps organizations proactively identify and address security issues, safeguard IoT assets, and preserve the dependability and integrity of IoT services. An approach for enhancing the security of Internet of Vehicles (IoV) systems through the creation of dynamic attack graphs using ontology-based techniques is in- troduced in [23]. To capture dynamic features of cyberattacks, such as conditional dependencies, time-sensitive actions, and the effect of countermeasures, the authors introduce a formal framework for building Dynamic Attack Trees [24]. With this method, it is easier to evaluate and respond to evolving real- world cyber threats.

In [26] provides a complex method of assessing cybersecurity risk through the use of dynamic attack graphs based on logic. These attack graphs offer a potent way to analyze and assess security risks in intricate computer systems. Dynamic logic-based attack graphs, as opposed to static attack graphs, can reflect the changing nature of cyberattacks by taking into consideration the actions of the attacker, vulnerabilities, and the long-term effects of security countermeasures. By enabling more precise and rapid assessments of potential threats and vulnerabilities, this dynamic approach improves risk assessment. As a result, the security posture of complex computer systems in the face of changing cyber hazards is eventually improved.

All the works in attack modeling mentioned above fail to address all the features of dynamic IoT networks. There is no proper explanation for generating new attack graphs over time. Incorporating XAI into attack modeling and addressing the dynamic nature of IoT networks aids defenders in identifying the root causes of vulnerabilities in each network scenario. Defenders can take specific action to address these changes in attack paths to prevent any further attacks.

III. ROLE OF XAI IN ATTACK MODELING FOR DYNAMIC IOT NETWORK.

a. Addressing the dynamicity of IoT network

In applications and situations where IoT devices and their interactions are frequently changing and where adaptability, scalability, and effective resource management are crucial, dynamic IoT networks are well suited. Realizing the full promise of IoT in fields like smart cities, industrial automation, and healthcare requires these networks. Some of the import- tant features of IoT networks are described below [25], [23], [27], [28], [29].

1. *Device Diversity:* IoT networks are made up of several types of devices, from basic sensors to strong gateways and edge devices, all with different kinds of capabilities. The vulnerabilities and weaknesses of various IoT devices can vary.
2. *Topological Changes:* Due to the mobility of devices or the addition/removal of devices, IoT network topologies can change regularly.
3. *Raising and patching of Vulnerabilities:* As few devices will be removed from the network some of the vulnerabilities will be patched over time. Similarly, when new devices are introduced into the network new vulnerabilities may arise.
4. *Change in connectivity:* When devices are joined and removed the connectivity between the devices will change according to the change in the firewall rules.
5. *Communication protocols:* In dynamic IoT networks, where devices might join, depart, or move within the network, require different communication protocols. For instance, a new IoT device can negotiate with the network infrastructure to choose the appropriate protocol for data exchange when it enters the network.

These key reasons make the dynamic IoT network crucial and thereby a different attack modelling strategy is needed. It is imperative to use XAI in attack modeling for IoT networks to improve the security of these networked systems.

B. Incorporating XAI in attack modeling

Dynamic IoT networks have a constantly changing network scenario, which frequently introduces new attack surfaces and attack paths [28]. So the network defenders should eagerly monitor for any change in the network. If the defender fails to identify any of the critical attack paths or provides incorrect countermeasures, the consequence will have far- reaching impacts. This is where XAI is required, XAI provides transparency and trust for identified attack paths and counter- measures.

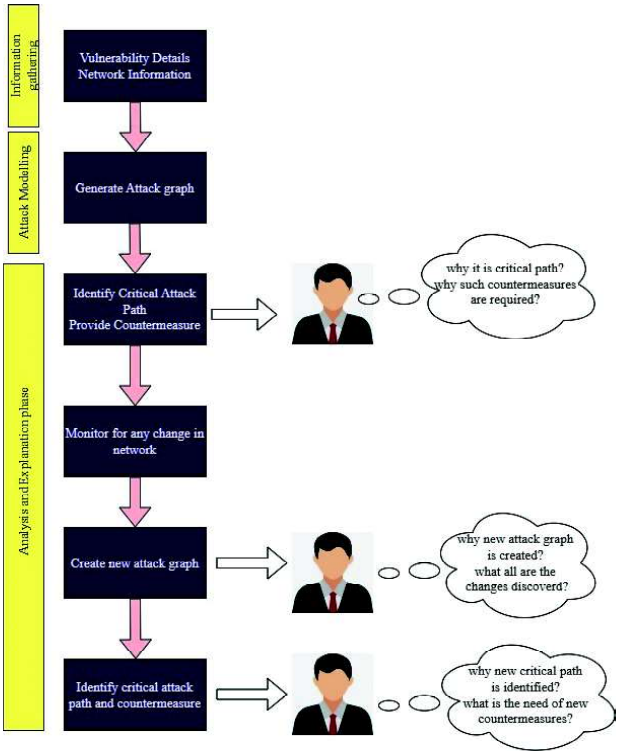
1. *Better Understanding of change in the network and attack graph:* The ML model will continuously monitor for the change in the network and if any changes are identified new attack graph is generated. XAI will explain the need for a new attack graph and what are the changes that occurred in the network and attack graph compared with the previously generated one.

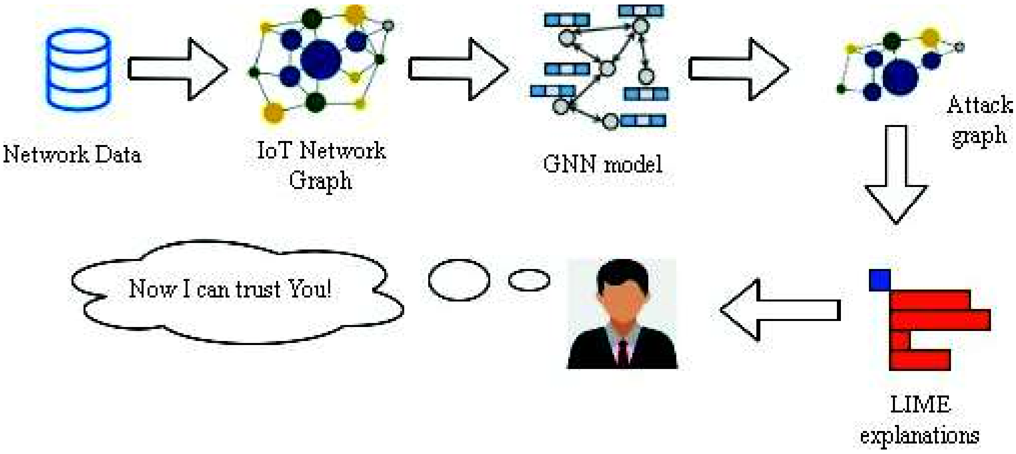
2. *Explainability regarding attack paths:* XAI will explain the reason for the existence of attack paths which is the most critical attack path and which features influenced the finding. With this explanation, the defenders will get a better knowledge of the possible attack scenarios which further helps in improving the security posture of the network.

3. *Transparency of countermeasures:* After the critical path is identified ML will provide suitable countermeasure strategies and the XAI will help to understand why a specific decision for a particular countermeasure is taken. It assists to discover and address potential problems with AI, such as accountability, bias, and discrimination.

IV. PROPOSED FRAMEWORK

We propose a new framework that uses Explainable AI to enhance transparency in the generated attack graph and countermeasures provided. Figure 1 shows the proposed framework.


Information gathering
Vulnerability Details Network Information
Attack Modelling
Generate Attack graph
Analysis and Explanation phase
Identify Critical Attack Path Provide Countermeasure
why it is critical path? why such countermeasures are required?
Monitor for any change in network
Create new attack graph
why new attack graph is created? what all are the changes discoverd?
Identify critical attack path and countermeasure
why new critical path is identified? what is the need of new countermeasures?



Our framework consists of three phases:

1. *Information Gathering:* The network is scanned to find any existing

vulnerabilities using network analyzer tools like Nessus, Retina, Open-VAS, and Nexpose. The information acquired in this initial stage offers a thorough picture of the system's resources, network layout, and potential vulnerabilities. The features and severity of the discovered vulnerabilities are then determined using the NIST Common Vulnerability Scoring System (CVSS) base metrics [32].

2. *Attack Modelling:* An IoT network graph is created with the data acquired in the information-gathering phase. Graph Neural Networks (GNNs) are appropriate for simulating attack pathways in network graphs as they can capture node and edge associations and are capable of learning the network structure information [31]. The graph's nodes and edges should include additional properties or attributes to provide the GNN with meaningful information for predicting attack paths. These attributes include device types, vulnerability information, firewall settings, and other relevant network information. Further GNN represents these predicted attack paths as an attack graph.

3. *Analysis and Explanation:* In this phase, the generated attack graph is used for the analysis and identification of critical attack paths. The reason for selecting an attack path as critical involves several reasons including the probability of attacker reachability, diversity of exploits in the paths, ease of exploiting vulnerabilities, and so on. With the help of the XAI LIME algorithm, we could get insights regarding why the path is critical, which are the appropriate countermeasure strategies to be applied, and why it is necessary to provide such countermeasures. Figure 2 shows the creation of the attack graph with GNN and LIME explanations.

Again in this phase, the framework monitors for any change in the network, the change can be identified via the parameters specified in section III A, if the change is noticed, a new attack graph is created and XAI will explain the changes that occurred and why the new graph is created. Again, from this newly created attack graph, the critical attack path in the attack graph is identified either with the help of any counting or difficulty-based metrics and further, the countermeasures are provided.

V. CASE STUDY

In our case study of the most popular IoT network which is Internet of Drones (IoD) network, a leader drone serves as a central node, managing communication with GCS and other IoD. Figure 3 shows the example IoD network. For effective data exchange and decision making, the leader drone can communicate with edge devices. Moreover, the network integrates edge computing capabilities, allowing edge devices to communicate with cloud services for secure storage of sensitive data.

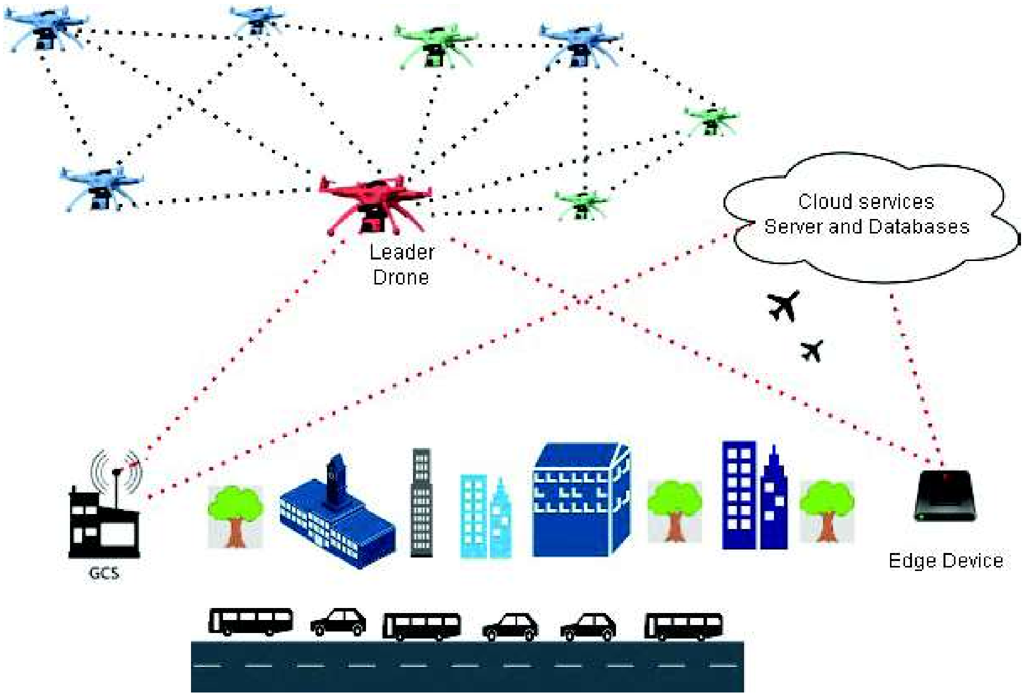


TABLE I

TOP FEATURES FOR IDENTIFYING NETWORK CHANGE

Features	Definition
firewall rules	Change in firewall rules of the network.
mobility	Mobility of Drone in the network.
protocol	Changes in the network protocols.
throughput	Change in throughput.
network density	Changes in the number of Drone in the IoD network.
topology change	Topological changes in the network.
latency	Change in latency.

Due to the absence of real-world data, we employed Monte Carlo simulation to generate a synthetic dataset. We validated the simulation process by comparing the results with established models to ensure that the approach is in line with pre- vailing best practices in IoD network analysis. Figure 6 shows the different possible attack paths from our IoD network. The features used for identifying the critical attack paths are shown in Table II.

TABLE II

TOP FEATURES FOR IDENTIFYING CRITICAL ATTACK PATH

Features	Definition
patch status	The existence of vulnerability in the network.
useraccess rights	Access rights of a user in the network.
cvss	Associated CVSS score for each vulnerability.
prob exploited	Probability of exploits being attacked.
diversity	Type of vulnerability in the attack path.
pathlength	Length of the attack path.
target	Attacker reachability to any of the targets in the network.

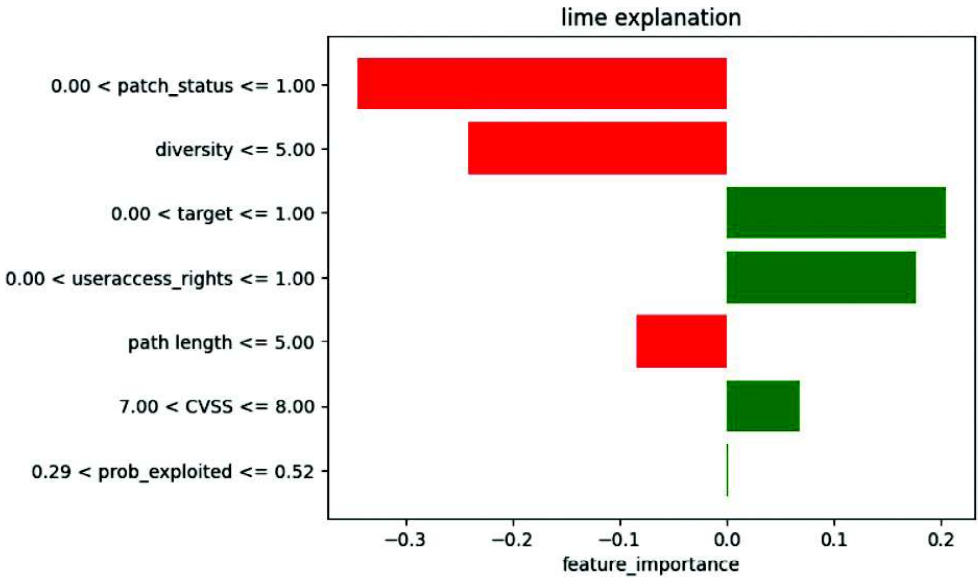


Fig. 4. Feature importance for predicting critical attack paths

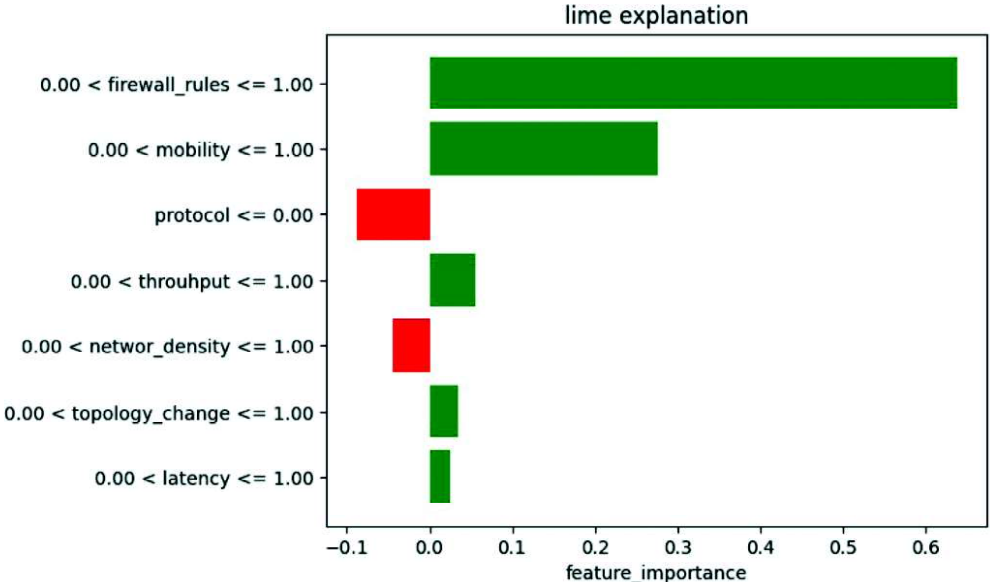


Fig. 5. Feature Importance for predicting network change

The importance of features contributing to the prediction is shown in Figure 4 is identified using LIME algorithm. The figure summarizes the high CVSS score, user access rights, target reachability, and the probability of exploitation as factors that positively contribute to predicting the specific path as crucial.

The model keeps monitoring the network for any change. LIME gives the importance of features contributing to identifying the change in the network. The features used for iden- tifying network change are shown in Table I. The importance of features that address the dynamicity is shown in Figure 5. Predicting network changes is aided by updates to firewall rules, the high mobility of Drone with topological changes, and variations in throughput and latency positively contribute to predicting network change.

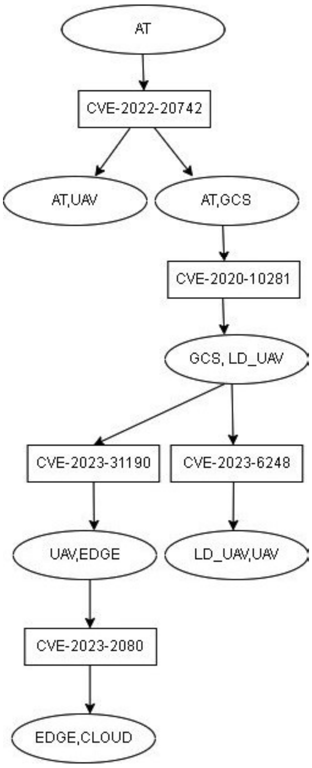


Fig. 6. Attack graph

As the network changes, the model continues to generate new attack graphs with explanations that assist in maintaining network security.

I. CONCLUSION AND FUTURE WORKS

It has become clear from our exploration of the dynamic and interconnected nature of IoT ecosystems that conventional security methods are insufficient to address the changing threat scenario. It is impossible to overestimate the importance of ML and DL for IoT security but there is a need for justifications for the decisions taken. In this conflict, XAI technologies have proven to be essential weapons, enabling us to identify threats and take action with unprecedented speed and accuracy. In a constantly changing network, XAI provides defenders with actionable information, transparency, and a deeper understanding of attack paths. Beyond technological advancement, the importance of securing IoT networks is fundamental to protecting key infrastructure, guaranteeing data privacy, and promoting confidence in the IoT's revolutionary potential. The paper will act as a starting point for further investigation, pushing the limits of what is feasible in the field of IoT security. We hope that this paper will encourage readers to learn more about this dynamic area, revealing fresh perspectives and stimulating new ideas that will continue to influence the development of secure IoT networks in the future.

REFERENCES

1. Al-Garadi, Mohammed Ali, et al. “A survey of the machine and deep learning methods for Internet of things (IoT) security.” IEEE Communications Surveys and Tutorials 22.3 (2020): 1646-1685.

2. Hassan, Rosilah, et al. “Internet of Things and its applications: A comprehensive survey.” Symmetry 12.10 (2020): 1674.

3. Pourhabibi, Tahereh, et al. “Fraud detection: A systematic literature review of graph-based anomaly detection approaches.” Decision Support Systems 133 (2020): 113303.

4. Sheyner, Oleg, and Jeannette Wing. “Tools for generating and analyzing attack graphs.” International symposium on formal methods for compo- nents and objects. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003.

5. George, Gemini, and Sabu M. Thampi. “Vulnerability-based risk as- sessment and mitigation strategies for edge devices in the Internet of Things.” Pervasive and Mobile Computing 59 (2019): 101068.

6. Jha, Somesh, Oleg Sheyner, and Jeannette Wing. “Two formal analyses of attack graphs.” Proceedings 15th IEEE Computer Security Founda- tions Workshop. CSFW-15. IEEE, 2002.

7. Schneier, Bruce. “Academic: Attack Trees—Schneier on Security.”

8. Kordy, Barbara, et al. “Attack–defense trees.” Journal of Logic and Computation 24.1 (2014): 55-87.

9. Brezolin, Uelinton, Andressa Vergu¨tz, and Michele Nogueira. “A method for vulnerability detection by IoT network traffic analytics.” Ad Hoc Networks 149 (2023): 103247.

10. Koppula, Manasa, and Leo Joseph LM. “LNKDSEA: Machine Learning Based IoT/IIoT Attack Detection Method.” 2023 International Con- ference on Advances in Electronics, Communication, Computing and Intelligent Information Systems (ICAECIS). IEEE, 2023.

11. Keserwani, Kushagra, Apoorva Aggarwal, and Anamika Chauhan. “At- tack detection in industrial IoT using novel ensemble techniques.” 2023 2nd International Conference on Vision Towards Emerging Trends in Communication and Networking Technologies (ViTECoN). IEEE, 2023.

12. Diro, Abebe Abeshu, and Naveen Chilamkurti. “Distributed attack detection scheme using deep learning approach for Internet of Things.” Future Generation Computer Systems 82 (2018): 761-768.

13. Abeshu, Abebe, and Naveen Chilamkurti. “Deep learning: The frontier for distributed attack detection in fog-to-things computing.” IEEE Com- munications Magazine 56.2 (2018): 169-175.

14. Sahu, Amiya Kumar, et al. “Internet of Things attack detection using hybrid Deep Learning Model.” Computer Communications 176 (2021): 146-154.

15. Marino, Daniel L., Chathurika S. Wickramasinghe, and Milos Manic. "An adversarial approach for explainable ai in intrusion detection systems." IECON 2018-44th Annual Conference of the IEEE Industrial Electronics Society. IEEE, 2018.

16. Forti, Stefano, Gian-Luigi Ferrari, and Antonio Brogi. "Secure cloud- edge deployments, with trust." Future Generation Computer Systems 102 (2020): 775-788.

17. Islam, Sheikh Rabiul, et al. "Domain knowledge aided explainable ar- tificial intelligence for intrusion detection and response." arXiv preprint arXiv:1911.09853 (2019).

18. Abou El Houda, Zakaria, Bouziane Brik, and Sidi-Mohammed Senouci. "A novel iot-based explainable deep learning framework for intrusion detection systems." IEEE Internet of Things Magazine 5.2 (2022): 20- 23.

19. Sheyner, Oleg, et al. "Automated generation and analysis of attack graphs." Proceedings 2002 IEEE Symposium on Security and Privacy. IEEE, 2002.

20. Payne, Josh, Karan Budhraja, and Ashish Kundu. "How secure is your iot network?." 2019 IEEE International Congress on Internet of Things (ICIOT). IEEE, 2019.

21. Wu, Runze, et al. "Network attack path selection and evaluation based on Q-learning." Applied Sciences 11.1 (2020): 285.

22. Chowdhary, Ankur, et al. "Autonomous security analysis and penetration testing." 2020 16th International Conference on Mobility, Sensing and Networking (MSN). IEEE, 2020.

23. Hou, Shuning, et al. "An ontology-based dynamic attack graph genera- tion approach for the internet of vehicles." Frontiers in Energy Research 10 (2022): 928919.

24. Ali, Aliyu Tanko, and Damas P. Gruska. "Dynamic Attack Trees." OVERLAY@ GandALF. 2021.

25. Alaba, Fadele Ayotunde, et al. “Internet of Things security: A survey.” Journal of Network and Computer Applications 88 (2017): 10-28.

26. Boudermine, Antoine, Rida Khatoun, and Jean-Henri Choyer. “Dynamic logic-based attack graph for risk assessment in complex computer systems.” Computer Networks 228 (2023): 109730.

27. Triantafyllou, Anna, Panagiotis Sarigiannidis, and Thomas D. Lagkas. “Network protocols, schemes, and mechanisms for internet of things (iot): Features, open challenges, and trends.” Wireless communications and mobile computing 2018 (2018).

28. Atlam, Hany F., et al. “Validation of an adaptive risk-based access control model for the internet of things.” International Journal of Computer Network and Information Security 12.1 (2018): 26.

29. Truong, Hong-Linh, Lingfan Gao, and Michael Hammerer. “Service architectures and dynamic solutions for interoperability of iot, network functions and cloud resources.” Proceedings of the 12th European Conference on Software Architecture: Companion Proceedings. 2018.

30. Zafar, Muhammad Rehman, and Naimul Khan. “Deterministic local interpretable model-agnostic explanations for stable explainability.” Ma- chine Learning and Knowledge Extraction 3.3 (2021): 525-541.

31. Jmal, Houssem, et al. “SPGNN-API: A Transferable Graph Neural Network for Attack Paths Identification and Autonomous Mitigation.” arXiv preprint arXiv:2305.19487 (2023).

32. P. Mell, K. Scarfone and S. Romanosky, “Common Vulnerability Scoring System,” in IEEE Security and Privacy, vol. 4, no. 6, pp. 85-89, Nov.- Dec. 2006, doi: 10.1109/MSP.2006.145.

***Blessy Thomas,** Connected Systems and Intelligence Lab, School of Computer Science and Engineering, Digital University Kerala, Technopark Phase IV, Thiruvananthapuram, Kerala, India. blessy.res21@duk.ac.in