ADVANCES IN COMPUTER ENGINEERING

EDITOR
PROF. SELMİN ENER RÜŞEN, PH.D.

DOI::10.5281/zenodo.14579277

Advances in Computer Engineering

EDITOR

Prof. Selmin Ener Rüşen, Ph.D.

Publisher
Platanus Publishing®

Editor in Chief
Prof. Selmin Ener Rüşen, Ph.D.

Cover & Interior Design
Platanus Publishing®

Editorial Coordinator
Arzu Betül Çuhacıoğlu

The First Edition
December, 2024

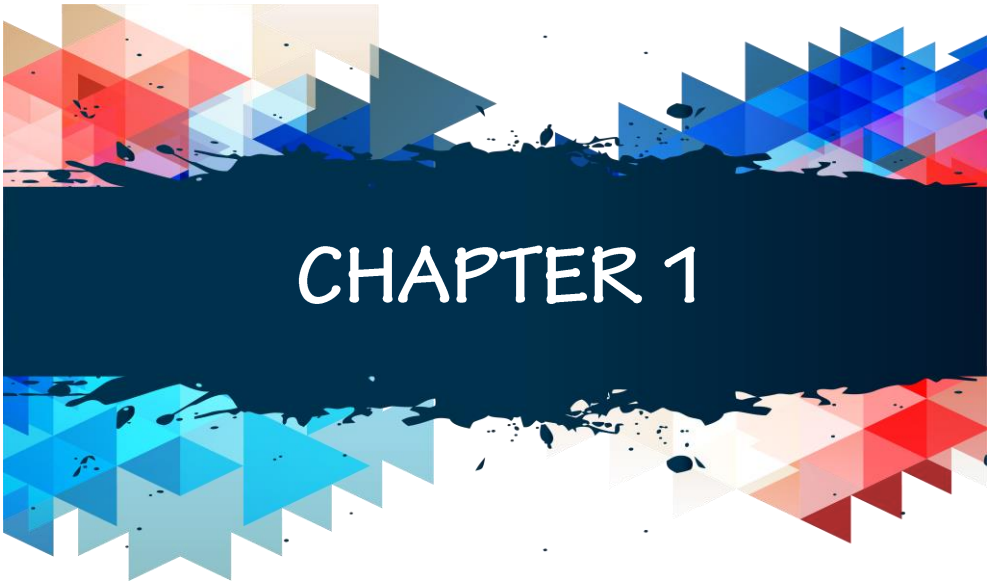
Publisher's Certificate No
45813

ISBN
978-625-6638-21-7

Platanus Publishing®
Address: Natoyolu Cad. Fahri Korutürk Mah. 157/B, 06480, Mamak, Ankara, Turkey.
Phone: +90 312 390 1 118
web: www.platanuskitap.com
e-mail: platanuskitap@gmail.com

PLATANUS PUBLISHING®

CONTENTS



Leveraging Machine Learning and Deep Learning for Enhanced User Review Classification

Mehmet Bilge Han Taş [1] ***& Eyyüp Yıldız*** [2]

[1] Res. Asst., Erzincan Binali Yildirim University, Faculty of Engineering and Architecture, Department of Computer Engineering, Erzincan, Turkey, ORCID: 0000-0001-6135-1849
[2] Asst. Prof. Dr., Erzincan Binali Yildirim University, Faculty of Engineering and Architecture, Department of Computer Engineering, Erzincan, Turkey, ORCID: 0000-0002-7051-3368

1. INTRODUCTİON

Sentiment analysis is an evaluation method used to classify and give an emotional result that a person has made from a written source [1]. Sentiment analysis has recently become widely used in the fields of artificial intelligence and robotics. Because many systems can be developed by perceiving the mood and emotions of the users. For example, many models can be designed and put into use, such as giving advertisements suitable for the mood, making music preferences, recommending movies that one wants to watch. Likewise, it has become very important to do sentiment analysis from texts. Because the spread of the internet and social media reaching every user, it has caused a tremendous increase in textual expressions. Thanks to the social media, which has become widespread in recent years and used by almost everyone, a very high amount of data has begun to form on the internet. It has become possible to establish a very wide sentiment analysis network in social media that companies will also benefit from. Comments and likes on products have become very important for companies to advertise or promote their products. They can use a wide range of reviews such as music, movies, hotels for holidays, books as products. In this way, while marketing their products, they can reach a wider audience in the light of this valuable data and can make an orientation in line with user requests.

Social media platforms and websites are vast user-generated content. Since it is used by many users, there is a wide variety of data entry. These data contain a wide range of ideas and opinions. Therefore, it is very important to evaluate these data. It is very important to use an automated evaluation system as the data is so large. Machine learning methods are very effective for understanding the ideas and emotional states of users. Therefore, its use has become very common in recent years.[2]. Different algorithms for data labeling and data manipulation Unigrams, Bigrams and N-grams are made with different techniques for data labeling. Machine learning methods are mostly used to generate positive or negative predictions as binary classification [3].

A supervised approach was used for use in the study. In this approach, a classification process was performed in the presence of labeled data [4]. There are tags for negative or positive user comments. These tags are created with the user ratings next to the comments made. Two types of labeling approaches have been made. By analyzing the user ratings of the data, the positive label was given to the comments with 7 points and above, and the negative label was given to the points below it. In the other approach, again looking at the distribution of scores,

it was labeled as positive above 7 points, neutral between 5.8-7 points and negative below 5.8 points. Machine learning techniques have been applied, with the second approach being multi-class.

In the study, machine learning methods and Convolutional Neural Network (CNN) were used for sentiment analysis and classification. The study was carried out to include a flow as follows.

- Sentiment analysis was made using hotel reviews. These data are taken from a publicly shared dataset available online. Preprocess operations were applied to this data set. Many features used for sentiment analysis were used while making transactions.
- The data set is divided according to user comments and given points. While doing this, a dual class label was created as positive-negative, and multiclass labeling was done as positive-neutral-negative for the other classification. Because there is no clear method to label a class without a label, two different methods have been classified as an interpretation of user scores.
- After separating the data set in two different ways, the data set was split as 70% train and 30% test. Machine learning and CNN models were applied and classification was made. Various optimization studies were made for the CNN model and the model was created in that way. Then, the results of the classes separated by the two methods were taken and compared.

In the study, the 515K Hotel Reviews Data in Europe data set on the Kaggle [5] site was used and sentiment analysis was made by applying artificial intelligence methods. This paper is organized as follows. In Section 2, studies related to the subject were examined. Section 3 gives information about the methods used for the study. In Section 4, the experimental results of the study are given. The results obtained in Section 5 were evaluated and critiqued. In Section 6, a general summary and conclusion evaluation has been made.

2. LİTERATURE REVİEW

Sentiment analysis was carried out using machine learning methods with a Lexicon-based approach. In the study, a five-class classification was made. KNN, Naive Bayes, Decision Tree, Random Forest were used as machine learning methods [6]. A lexicon-based approach is preferred in Tamil texts. Bag of word and k-means were used. A 79% classification success was found using traditional

methods such as TD-IDF and word count, point count [7]. In this study, the comments of some products were examined and these products were classified. By using machine learning methods, a success rate of over 90% has been achieved for each classification. The highest was achieved with the Naive Bayes method with a success rate of 98% [8]. For e-commerce sites, a review was made according to the age and gender characteristics of the users. The data set was used by collecting book reviews on Facebook. In addition to machine learning methods, convolutional neural network was also used in the study. All results have been compared. A success of around 80% has been achieved with the CNN model [9]. Sentiment analysis was carried out using the Twitter data set. In this study, neural networks and machine learning methods were used. F1-score, recall and precision values were used as evaluation metrics. Four classes were determined by analysis. These are Strongly positive, Strongly negative, Mildly positive and Mildly negative. In general, metric values over 90% were found [10].

The studies with 515K Hotel Reviews Data in Europe, which is the data set used in the study, are as follows. In this study, an approach was made with LSTM. Machine learning methods have been applied. Results were found with dual class and triple class. The highest results were found as accuracy of 97%, F1-score 76.53%, precision 83%, recall 71% [11]. By using deep learning methods, results were tried to be obtained in double and quadruple classes. Grades were assigned as best for scores above 7, good for scores of 5-7, bad for scores between 3-5, and worst for scores below 3. It is not shown how these criteria were made. As a result of the study, precision, recall and F1-score values were obtained over 92% [12]. In this study, it was done by machine learning method. In the study, 7 models were considered within the framework of the preprocessing method according to many situations. Accuracy was used as the evaluation metric in the study. In the experimental results, it is seen that the best method is found in model 6 with SVM [13].

3. MATERİAL AND METHOD

In this section, the methods applied in the study are given. The studies were basically implemented with two different methods. While a two-class study was conducted in the first method, a three-class study was carried out in the second method. The flow chart of the study is given in Figure 1. First, the data set [5] was taken. Then, the data set was subjected to a certain pre-processing process. Then the data was split as 70% train and 30% test. Training was carried out with machine learning and CNN methods. The results obtained; It has been compared with evaluation metrics such as accuracy, precision, recall, f1-score and the process is finished with the model.

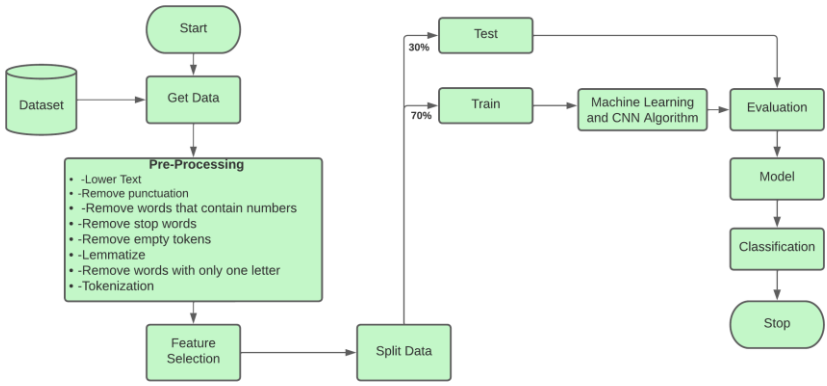


Figure 1. Flow chart of the study for sentiment analysis

3.1 Dataset

The dataset is a very large dataset consisting of 515 thousand customer comments. Each row contains 17 attributes of users and hotel information. In the study, a classification process was made by taking the user comments and the scores given by the users to the hotels. Distribution functions are given in Figure 2.

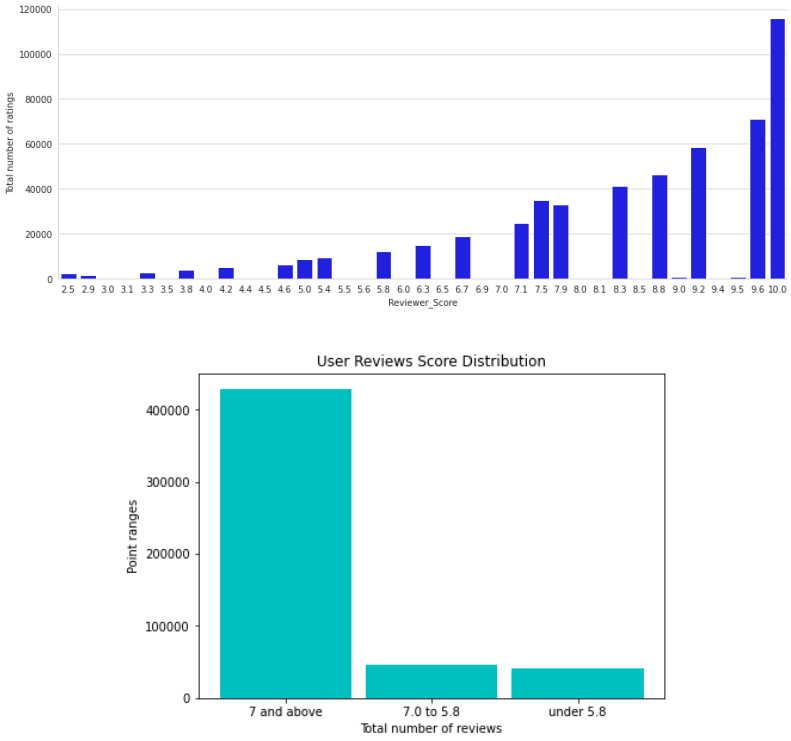


Figure 2. Distribution of points given by users

There are many attributes in the data set, such as the location of the hotels, the countries they are located in, and the length of the words. However, only the user comments and the scores they gave were discussed in order to make sentiment analysis. In addition, classification distributions were made according to the distribution given in Figure 2. In the first classification process, positive class was given above 7 scores and negative below. In the other classification, considering the various distributions, positive classes above 7, neutral between 5.8-7 and negative classes below 5.8 points were given.

3.2 Pre-Processing

Lowercase converts all words in the dataset to lowercase. In this way, the weights of the words will be the same and their domains will not have changed. If the same expression is written in capital letters elsewhere, it will have the same effect. If these words are not reduced to the same size, their domains will have changed [14-16]. Stopwords are words that are used functionally in sentences but have no effect on sentiment analysis. Every language has its own stopwords. Because they are often found in sentences, they can weight weights incorrectly [17].

So it would be more convenient to remove it. Punctuation remove and number remove are the removal of punctuation marks. Because punctuation does not contain emotion, it is usually removed in analysis studies [14]. Lemmatization is used to take root words [18]. Many languages contain words in additive form. Word parts that add emotion are usually determined from the roots. The appendices are removed as they may distort this weighting. Tokenization is used to divide sentences into more meaningful units. In this way, domains of influence can be revealed. It is very widely used in NLP.

3.3. Algorithms Used in the Study

3.3.1. Logistic Regression (LR)

Logistic regression is used to find probabilities of multiple dependent variables. It is also used for dependent and independent variables. Its main purpose is to analyze all variables and give a simple output [19]. It is widely used in large-scale data sets due to its high performance and fast operation. It is seen that it gives good results when it is a correlative structure. This method used in the study was used for both methods. It is known that it works better than linear regression when there is a curvilinear distribution. As the number of data increases, the curvature and distribution will increase, so it is considered to be suitable for this data set.

3.3.2. Decision Tree (DT)

Decision tree is a machine learning algorithm that belongs to supervised learning algorithms. It is used to solve classification problems [20]. In this study, a decision tree classifier is used to estimate the dependent variable based on some derived decision rules from previous data (training and testing phases). It is represented as nodes and nodes where root nodes are used to classify the properties of the instances. Leaf nodes (nodes without children) represent decisions or classifications. Evaluating the highest gain (most homogeneous branches) among all other features at each stage is the basic choice of a decision tree at each node. The performance of the decision tree is evaluated using a confusion matrix [21]. Mathematically Entropy for multiple attributes is represented as:

$$E(T, X) = \sum_{c \in X} P(c)E(c) \quad (1)$$

3.3.3. Random Forest (RF)

Random forest classifier was used as the classification method. The random forest classifier consists of a combination of tree classifiers, in which each classifier is constructed using a random vector sampled independently of the input vector, and each tree gives a unit vote for the most popular class to classify an input vector, i.e. counts [22]. The design of a decision tree requires the selection of a feature selection measure and pruning method. There are many approaches to the selection of features used for decision tree induction, and most approaches directly add a measure of quality to the attribute. The most frequently used attribute choices in decision tree induction are the information gain ratio criterion [23] and the Gini Index [24]. The random forest classifier uses the Gini Index as an attribute selection measure that measures the impurity of attributes by classes. In short, the random forest classifier travels through the forests, making a progression towards the branches. When it reaches the end of the branches, it makes a vote. Here, n denotes the number of trees to be visited. For example, if we choose n as 5, the result is drawn from among 5 trees and a vote is made. As a result of voting, the most voted class or prediction result is obtained. In this way, a successful prediction or result opportunity is caught.

3.3.4. Naive Bayes (NB)

Naive Bayes assigns the most probable value in a sample space for feature extraction. The properties in the sample are treated as being independent of the given class and can be made very simple. Although it does not work very well in theory, it is seen that it gives better results than many classifiers in practice [25]. It is based on a simple mathematical calculation and is as follows;

$$P(c|x) = \frac{P(c|x)P(c)}{P(x)} \quad (2)$$

The class's prediction probability is P(c|x). The class's prior probability is P(c). The probability of the class estimator is P(x|c), which is the probability. The estimator's prior probability is P(x). If a new sample is encountered, the class with the highest probability is found by considering the probability values calculated in finding the membership probability of this sample [26]. No estimation is made for a data in the test set if there is no counterpart in the training set. A straightforward yet effective approach for predictive modeling is the Naive Bayes method. Even with few data, it has great predictive power. Because of these beneficial and useful characteristics, it is a classifier that is preferred and used in many

fields. A modest yet effective approach for predictive modeling is the Naive Bayes method. Even with few data, it has great predictive power. Because of these beneficial and useful characteristics, it is a classifier that is preferred and used in many fields [27].

3.3.5. K-Nearest Neighbor (KNN)

K-nearest neighbor (K-NN) is a widely used classifier in classification [28]. It basically develops an estimate by interacting with neighbors around a certain diameter in the dataset. The larger the diameter, the more likely the features will be lost. Therefore, it is very important to use it at the optimum level when determining the number of neighbors. K-Nearest Neighbor (KNN) classifier; The KNN algorithm is a widely used method in data mining. K-Nearest Neighbors (kNN) is a simple but effective non-parametric classification method in many situations. To classify a t data record, the k nearest neighbors are taken and this creates a neighborhood of t. Majority voting among neighborhood data records is often used to decide classification for t, with or without distance-based weighting [29]. In the study, KNN was used so that it can be used in comparison, even though it has a high time cost.

3.3.6. XGBoost (XGB)

Xgboost [30], developed by Chen et al., is an efficient and scalable implementation of the gradient boosting framework [31, 32]. It has a tree learning-based structure. It has a linear solve function and it tries to increase low values in particular and it has a structure that allows this within the tree. It is a widely used and functional method with uses such as classification and regression. Since the packages applied are in an extensible state, it is possible to make an application for every problem. It has been used a lot in recent years because it generally shows high performance in machine learning algorithms. Therefore, this classifier is also used to compare and get results.

3.3.7. Convolutional Neural Network (CNN)

CNN models are usually created in 2D. However, in recent years, 1D CNN models, which are a modified version, have also been used [33, 34]. In terms of computational complexity, 1D CNN models are lower than 2D CNN models. Therefore, fast results can be obtained. Due to their working performance, they can be modeled to fit the data set [35]. 1D CNN model was used in the proposed study. Because the data set to be classified consists entirely of numbers. Because

while feature selection is made in NLP applications, textual expressions are converted to numerical weights and therefore the dataset to be used is digitized. The general architecture of the 1D CNN model is given in Figure 3.

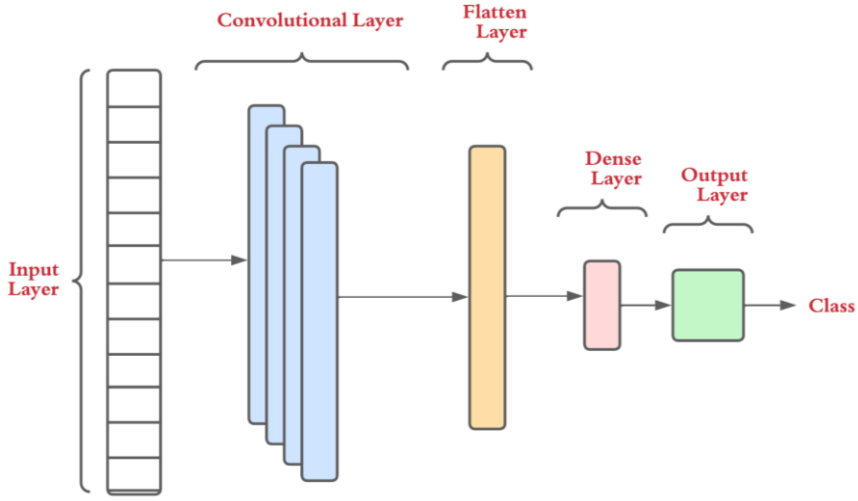


Figure 3. An exemplary 1D CNN architecture

Many models have been tried in the study, and the model with the best results is as in Figure 4. The input value from the dataset enters the CNN network. Then MaxPooling1D is applied by entering the Conv1D network. Finally, an output is obtained by passing through the Flatten and Dense layers.

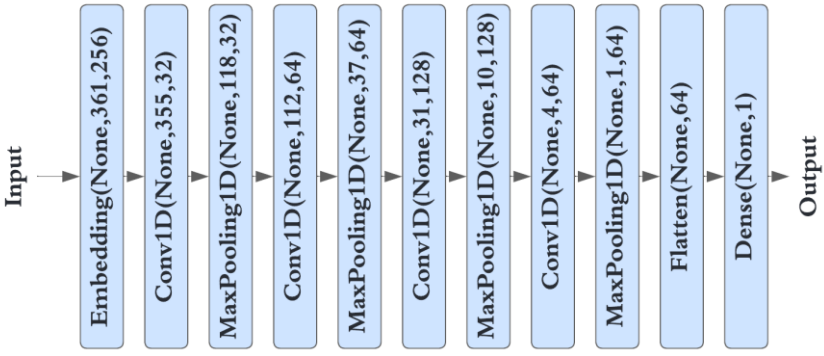


Figure 4. 1D CNN Model used in the study

3.4. Evaluation Metrics

In order to compare the results of the study, some evaluation metrics are needed. In this way, the accuracy of the study and the superiority of machine learning methods to each other will be seen. Experimental results will reveal the final best performances within this framework. The metrics used in the study are as follows;

$$Accuracy = \frac{TP + TN}{TP+FP+TN+FN} \quad (3)$$

$$F1 - score = \frac{2 * Precision * Recall}{Precision + Recall} \quad (4)$$

$$Precision = \frac{TP}{TP+FP} \quad (5)$$

$$Recall = \frac{TP}{TP+TN} \quad (6)$$

Accuracy (4) is the quotient of correctly predicted results and all results, which actually means overall performance. F1-score (5) expresses the harmonic mean between precision and recall values. Precision (6) gives the ratio of true positive results to other positive results. Recall (7) value is the ratio of true positive values to true negative and true positive values [36]. Confusion Matrix must be created to calculate all these metrics.

4. EXPERIMENTS AND RESULTS

In this section, the results of the experimental studies are given. Results As mentioned in the previous sections, two different results are given for two-class and multi-class results. In order to compare the results, accuracy, precision, recall and f1-score values were used as evaluation metrics. Before the study, pre-processing processes were carried out. The dataset is split into 70% train and 30% test. Then, the results were obtained by applying machine learning algorithms and CNN model to the data set.

Figure 5. Two-class machine learning methods confusion matrices

We need confusion matrix to calculate the accuracy of the classes as a result of machine learning methods. For this reason, it is necessary to make separate calculations for both two-class and multi-class. Figure 5 has a confusion matrix for the two-class. With the values obtained from here, accuracy, precision, recall, f1-score evaluation metrics can be calculated.

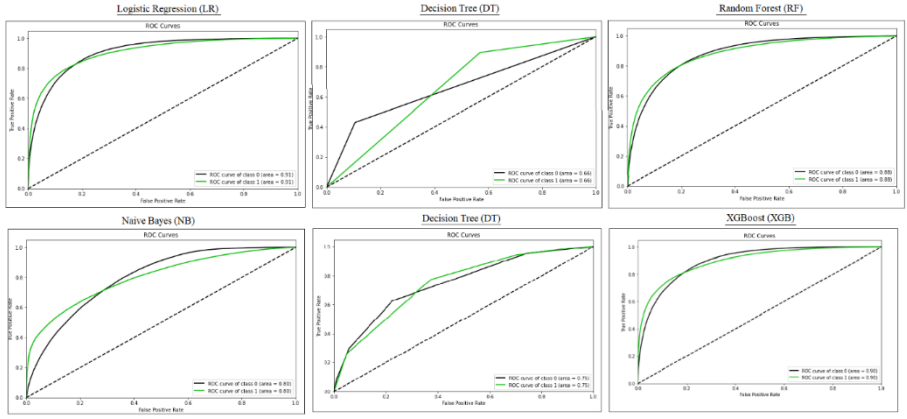


Figure 6. Two-class machine learning methods ROC Curves

ROC Curve, on the other hand, are metrics that show how well the model works after applying machine learning techniques. These metrics show us how well the data is performing. The closer the classes are to 1 the better, the closer to 0 the worse.

The final results and comparison are available in Table 1 and Table 2. There is a two-class structure. While Table 1 has results weighted by the number of classes, Table 2 shows the highest results achieved by any class.

Table 1. Two-class machine learning methods experimental weighted results of classes

ML Algorithm	Accuracy	Precision	Recall	F1-score	ROC
LR	**88%**	**87%**	**88%**	**87%**	**91%**
DT	81%	81%	81%	81%	66%
RF	85%	84%	85%	80%	88%
NB	80%	81%	80%	80%	80%
KNN	83%	81%	83%	81%	75%
XGB	**88%**	**87%**	**88%**	86%	90%

Table 2. Two-class machine learning methods experimental maximum results of classes

ML Algorithm	Accuracy	Precision	Recall	F1-score	ROC
LR	**88.2%**	**90.3%**	96.0%	**93.1%**	**91%**
DT	81.5	88.4	89.4	88.9	66%
RF	84.6	84.7	**99.4**	91.4	88%
NB	79.6	89.1	85.9	87.5	80%
KNN	83.2	86.7	94.2	90.3	75%
XGB	87.7	89.2	96.8	92.9	90%

We need confusion matrix to calculate the accuracy of the classes as a result of machine learning methods. For this reason, it is necessary to make separate calculations for both two-class and multi-class. Figure 7 has a confusion matrix for the multi-class. With the values obtained from here, accuracy, precision, recall, f1-score evaluation metrics can be calculated.

In the confusion matrix shown in Figure 7, multi-class results can be seen. Thanks to this matrix, performances are calculated and reflected in the result in this way.

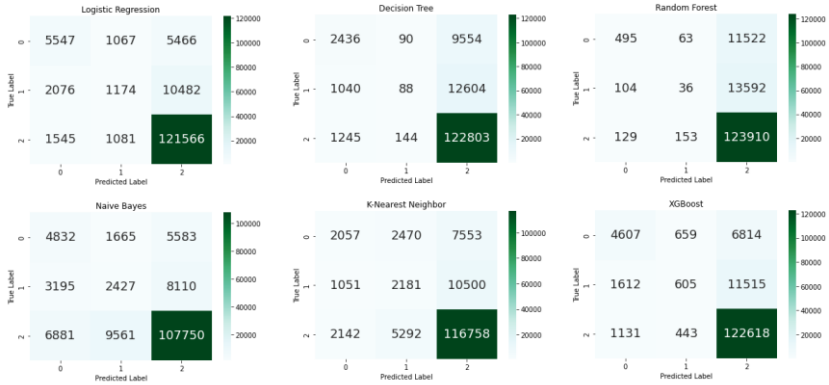


Figure 7. Multi-class machine learning methods confusion matrix

ROC Curve, on the other hand, are metrics that show how well the model works after applying machine learning techniques. These metrics show us how well the data is performing. The closer the classes are to 1 the better, the closer to 0 the worse. The ROC Curves of each class were drawn differently, in accordance with the multi-class structure of the results. Because the classes are not numerically equal to each other. Even with the same number of classes, the results may differ. That's why each is drawn separately. In Figure 8, curves for each of the 3 classes are given.

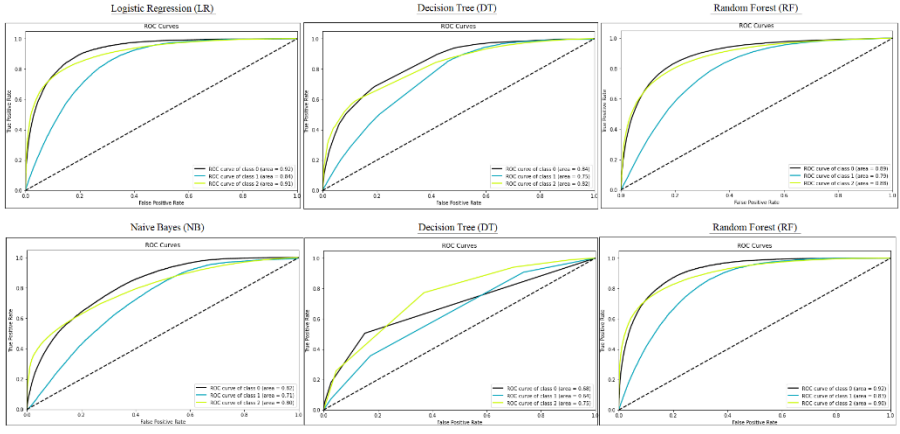


Figure 8. Multi-class machine learning methods ROC Curves

The final results and comparison are available in Table 3 and Table 4. There is a two-class structure. While Table 3 has results weighted by the number of classes, Table 4 shows the highest results achieved by any class.

Table 3. Multi-class machine learning methods experimental weighted results of all classes

ML Algo-rithm	Accuracy	Precision	Recall	F1-score	ROC
LR	**86%**	**81%**	**86%**	**82%**	**90%**
DT	84%	77%	84%	78%	82%
RF	83%	76%	83%	76%	87%
NB	77%	78%	77%	77%	79%
KNN	81%	77%	81%	78%	73%
XGB	85%	80%	85%	81%	**90%**

Table 4. Multi-class machine learning methods experimental maximum results of all classes

ML Algo-rithm	Accuracy	Precision	Recall	F1-score	ROC
LR	**85.5%**	**81.3**	**85.5**	**82.4**	**90%**
DT	83.5	76.8	83.5	78.0	82%
RF	83.0	75.6	83.0	75.8	87%
NB	76.7	77.7	76.7	77.1	79%
KNN	80.7	76.9	80.7	78.2	73%
XGB	85.2	80.3	85.2	81.1	**90%**

Machine learning techniques have been applied and the results are given above. No parameter optimization has been made in machine learning methods. Results were obtained with default values. Evaluation of the results was done in other sections.

CNN model accuracy and loss values are given in Figure 9. Many parameter values were tried while the model was being set up. These values were taken as a result of the operations performed with the highest and stable values. Train accuracy was up to 98.4%, while validation accuracy was up to 89%. Loss values

are below 1% for both. As the activation function, ReLU [37] in the CNN layer and sigmoid in the Dense layer are used. Adamax [38] was used as the optimizer. Binary_crossentropy was used as the Loss function and a total of 20 epochs were applied.

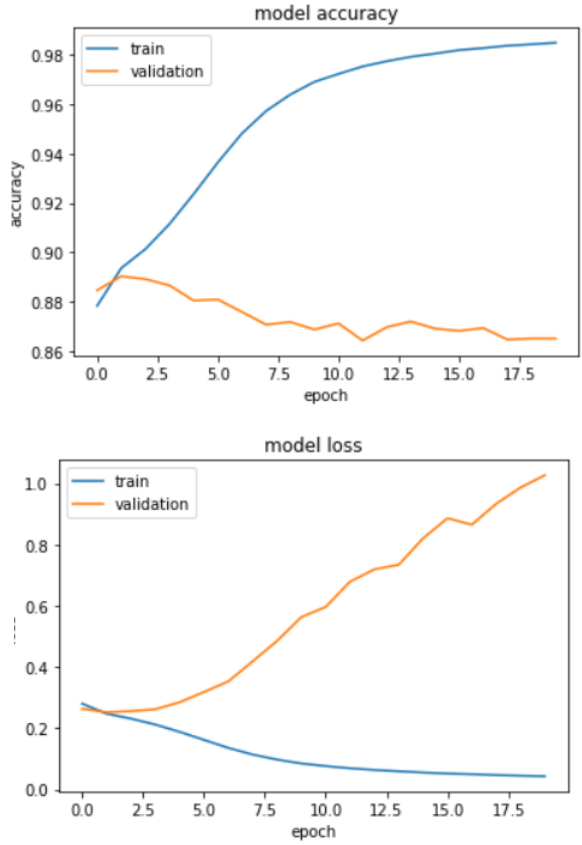


Figure 9. Model accuracy and loss values of CNN Model

5. DISCUSSION

The study was conducted on the "515K Hotel Reviews Data in Europe" dataset obtained from the Kaggle website. In the study, sentiment analysis was made. The pre-processing process, which is one of the most important parts of the sentiment analysis, has been done. The data were split as 70% train and 30% test. Classes are divided according to user scores in order to perform the classification process. These classes are handled in two different ways as double and triple.

Then, Logistic Regression, Decision Tree, Random Forest, Naive Bayes, K-Nearest Neighbor and XGBoost machine learning techniques were applied one by one. 1D Custom CNN Model has been proposed and a success has been achieved. The best weighted results for the two-class; 88% accuracy (LR), 87% precision (XGB), 88% recall (LR), 87% f1-score (LR), 91% ROC-score (LR) values were taken. The highest class results achieved were 88.2% accuracy (LR), 90.3% precision (LR), 99.4% (RF), 93.1% f1-score (LR) , 91% ROC-score (LR) values. The results of Logistic Regression were very good in both classification structures. For multi-class; 86% accuracy (LR), 81%precision (LR), 86% recall (LR), 82% f1-score (LR), 90% ROC-score (LR) values were taken. The highest class results achieved were 85.5% accuracy (LR), 81.3% precision (LR), 85.5% (RF), 82.4% f1-score (LR), 90% ROC-score (LR). For multi-class, Logistic Regression is at the forefront. As a result of both evaluations, the highest accuracy value was the custom CNN model with 89%.

6. SUMMARY AND CONCLUSION

In the study, many articles related to sentiment analysis were examined. In the light of this information, the methods were determined. Especially when using pre-processing and machine learning techniques, previous studies are based on. After the work flow was determined, very long processing times were compared in the sentiment analysis study of very large data. This shows that as the data grows, computers with high processing capacity are needed. Since the positive user scores in the data set are very intense, it can be said that the weighted results are more accurate. Because the data stacked in a certain place does not show the deviations very well. The reason why the data set is separated in different ways is to show more realistic performances by distributing this weight to other classes. With this study, companies and users can evaluate and develop based on user comments. These methods can also be applied to other datasets related to sentiment analysis and can get similarly successful and satisfactory results.

REFERENCES

[1] R. J. C. o. t. A. Feldman, "Techniques and applications for sentiment analysis," vol. 56, no. 4, pp. 82-89, 2013.

[2] M. Ahmad, S. Aftab, S. S. Muhammad, and S. J. I. J. M. S. E. Ahmad, "Machine learning techniques for sentiment analysis: A review," vol. 8, no. 3, p. 27, 2017.

[3] H. Wang, D. Can, A. Kazemzadeh, F. Bar, and S. Narayanan, "A system for real-time twitter sentiment analysis of 2012 us presidential election cycle," in *Proceedings of the ACL 2012 system demonstrations*, 2012, pp. 115-120.

[4] P. Gonçalves, M. Araújo, F. Benevenuto, and M. Cha, "Comparing and combining sentiment analysis methods," in *Proceedings of the first ACM conference on Online social networks*, 2013, pp. 27-38.

[5] Kaggle, "515K Hotel Reviews Data in Europe, https://www.kaggle.com/datasets/jiashenliu/515k-hotel-reviews-data-in-europe (Last Access: 26.06.2022)," 2017.

[6] A. J. J. o. U. C. Mitra and C. Technologies, "Sentiment analysis using machine learning approaches (Lexicon based on movie review dataset)," vol. 2, no. 03, pp. 145-152, 2020.

[7] S. Thavareesan and S. Mahesan, "Sentiment analysis in Tamil texts: A study on machine learning techniques and feature representation," in *2019 14th Conference on Industrial and Information Systems (ICIIS)*, 2019, pp. 320-325: IEEE.

[8] R. S. Jagdale, V. S. Shirsat, and S. N. Deshmukh, "Sentiment analysis on product reviews using machine learning techniques," in *Cognitive informatics and soft computing*: Springer, 2019, pp. 639-647.

[9] S. Kumar, M. Gahalawat, P. P. Roy, D. P. Dogra, and B.-G. J. E. Kim, "Exploring impact of age and gender on sentiment analysis using machine learning," vol. 9, no. 2, p. 374, 2020.

[10] M. Ghiassi and S. J. E. S. w. A. Lee, "A domain transferable lexicon set for Twitter sentiment analysis using a supervised machine learning approach," vol. 106, pp. 197-216, 2018.

[11] A. Ishaq *et al.*, "Extensive hotel reviews classification using long short term memory," vol. 12, no. 10, pp. 9375-9385, 2021.

[12] S. R. J. R. J. C. S. Labhsetwar, "Sentiment analysis of customer satisfaction using deep learning," vol. 6, pp. 709-715, 2019.

[13] D. Campos, R. R. Silva, and J. Bernardino, "Text Mining in Hotel Reviews: Impact of Words Restriction in Text Classification," in *KDIR*, 2019, pp. 442-449.

[14] K. J. E. S. w. A. Kim, "An improved semi-supervised dimensionality reduction using feature weighting: Application to sentiment analysis," vol. 109, pp. 49-65, 2018.

[15] B.-T. Nguyen-Thi and H.-T. Duong, "A Vietnamese sentiment analysis system based on multiple classifiers with enhancing lexicon features," in *International Conference on Industrial Networks and Intelligent Systems*, 2019, pp. 240-249: Springer.

[16] A. Tagarelli and H. Tong, *Computational Data and Social Networks: 8th International Conference, CSoNet 2019, Ho Chi Minh City, Vietnam, November 18–20, 2019, Proceedings*. Springer Nature, 2019.

[17] H.-T. Duong and T.-A. J. C. S. N. Nguyen-Thi, "A review: preprocessing techniques and data augmentation for sentiment analysis," vol. 8, no. 1, pp. 1-16, 2021.

[18] S. Pradha, M. N. Halgamuge, and N. T. Q. Vinh, "Effective text data preprocessing technique for sentiment analysis in social media data," in *2019 11th international conference on knowledge and systems engineering (KSE)*, 2019, pp. 1-8: IEEE.

[19] S. J. B. m. Sperandei, "Understanding logistic regression analysis," vol. 24, no. 1, pp. 12-18, 2014.

[20] S. R. Safavian, D. J. I. t. o. s. Landgrebe, man,, and cybernetics, "A survey of decision tree classifier methodology," vol. 21, no. 3, pp. 660-674, 1991.

[21] Y. K. Qawqzeh, M. M. Otoom, F. Al-Fayez, I. Almarashdeh, M. Alsmadi, and G. J. I. Jaradat, "A proposed decision tree classifier for atherosclerosis prediction and classification," vol. 19, no. 12, p. 197, 2019.

[22] L. J. U. o. C. B. Breiman, CA, USA, "Random Forests; UC Berkeley TR567," 1999.

[23] J. R. Quinlan, *C4. 5: programs for machine learning*. Elsevier, 2014.

[24] L. Breiman, J. Friedman, R. Olshen, and C. J. B. R. Stone, Florida, "Classification and regression trees–crc press," 1984.

[25] I. Rish, "An empirical study of the naive Bayes classifier," in *IJCAI 2001 workshop on empirical methods in artificial intelligence*, 2001, vol. 3, no. 22, pp. 41-46.

[26] E. Frank and R. R. Bouckaert, "Naive bayes for text classification with unbalanced classes," in *European Conference on Principles of Data Mining and Knowledge Discovery*, 2006, pp. 503-510: Springer.

[27] Ö. ŞAHİNASLAN, H. DALYAN, and E. J. B. T. D. ŞAHİNASLAN, "Naive Bayes Sınıflandırıcısı Kullanılarak YouTube Verileri Üzerinden Çok Dilli Duygu Analizi," vol. 15, no. 2, pp. 221-229, 2022.

[28] Y. Wu, K. Ianakiev, and V. J. P. r. Govindaraju, "Improved k-nearest neighbor classification," vol. 35, no. 10, pp. 2311-2318, 2002.

[29] G. Guo, H. Wang, D. Bell, Y. Bi, and K. J. L. N. i. C. S. Greer, "Ontologies, Databases, and Applications of Semantics (ODBASE) 2003 International Conference-Data Semantics and Metadata-KNN Model-Based Approach in Classification," vol. 2888, pp. 986-996, 2003.

[30] T. Chen *et al.*, "Xgboost: extreme gradient boosting," vol. 1, no. 4, pp. 1-4, 2015.

[31] H. T. Friedman J, Tibshirani R, et al. , "“Additive logistic regression: a statistical view of boosting (with discussion and a rejoinder by the authors).”," *The annals of statistics, 28(2),* pp. 337–407, 2000.

[32] J. H. Friedman, "Greedy function approximation: a gradient boosting machine," *Annals of Statistics,* pp. 1189-1232, 2001.

[33] S. Kiranyaz, T. Ince, O. Abdeljaber, O. Avci, and M. Gabbouj, "1-D convolutional neural networks for signal processing applications," in *ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2019, pp. 8360-8364: IEEE.

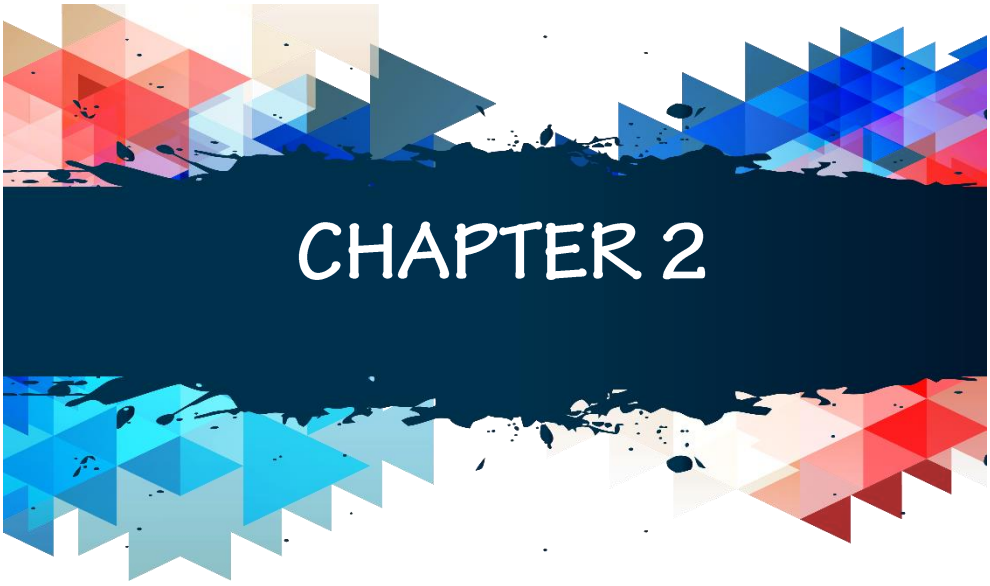
[34] L. Eren, T. Ince, and S. J. J. o. S. P. S. Kiranyaz, "A generic intelligent bearing fault diagnosis system using compact adaptive 1D CNN classifier," vol. 91, no. 2, pp. 179-189, 2019.

[35] S. Kiranyaz *et al.*, "1D convolutional neural networks and applications: A survey," vol. 151, p. 107398, 2021.

[36] M. Hossin, M. N. J. I. j. o. d. m. Sulaiman, and k. m. process, "A review on evaluation metrics for data classification evaluations," vol. 5, no. 2, p. 1, 2015.

[37] J. H. J. T. a. o. s. Friedman, "Multivariate adaptive regression splines," vol. 19, no. 1, pp. 1-67, 1991.

[38] D. P. Kingma and J. J. a. p. a. Ba, "Adam: A method for stochastic optimization," 2014.



A Survey of the Analysis of Link Prediction Based on Complex Networks

***Serpil Aslan*[1]**

[1] Assoc. Prof. Dr., Malatya Turgut Ozal University, Department of Software Engineering, Faculty of Engineering and Natural Sciences, ORCID: 0000-0001-8009-063X

1. Introduction

Network theory is an interdisciplinary science that offers various approaches to understanding the interactions between different entities in complex systems. Networks are widely used to represent various real-world systems, such as social, biological, and technological information systems in nature and society. Social networks, which have become the focus of interest for many researchers working in different disciplines, have a highly dynamic and complex structure. Social Network Analysis (SNA) is a broad research area that tries to cope with this complexity [1]. In social networks, changes can occur in the topological structure of the network over time, both by adding new edges and new nodes or by removing existing edges or nodes. Link prediction, one of the most critical areas of social network analysis research, deals with changes in the state of the links that occur due to these changes in the network. Link prediction is widely used in many fields [2]. For example, it conducts research in a wide variety of fields not limited to network science, such as bibliographic field [3], biology analysis [4], recommendation systems [5,6,7], and other hot fields.

Liben-Nowell et al. [7] addressed the problem of link prediction and various similarity measures. To date, many approaches have been presented to address this problem. In the literature, commonly used metrics for link prediction in social networks can be categorized as semantic and topological-based metrics [8]. The number of familiar neighbors between two nodes is an example of a topological metric. Unlike topological metrics, semantic metrics use the content of nodes to calculate the similarity between nodes. The general idea for both similarity metrics is that node pairs with high similarity metrics are more likely to be connected. Topological metrics are categorized as neighborhood-based and path-based metrics [9]. Neighborhood-based metrics consider the neighbors of a node. According to this metric, the higher the number of familiar neighbors of two nodes, the more likely there will be future connections between the node pairs. Path-based metrics consider the paths between the node pairs [10]. The basic logic of this measure is that the probability of future connections between pairs of nodes is directly proportional to the shortness of the paths between them. However, most of the closeness measures adopted in the literature use the network data statically without considering the network's evolutionary development. However, when the evolutionary development of the network is analyzed, it is seen that some exceptional cases occur between pairs of nodes. A new connection may form between two pairs of nodes that are not connected in a specific time interval of the network in the next interval, or the connection between two connected nodes may disappear in the next time interval. With the addition of new nodes and connections to

the network, the connection strength between the pairs of nodes may increase or vice versa decrease. This situation represents the development of the relevant social network. Undoubtedly, the evolutionary development of social networks is a high-potential source of information for link prediction. For this reason, the evolutionary development of the network is an important issue to be considered during link prediction [9].

Most scientific studies in the field of social networks focus on the analysis of single-part networks. However, many complex networks created from real-world data have a two-part structure. For this reason, single-part networks can often be inadequate when representing real-world systems. Two-part networks are a particular type of network that represents interactions between different groups of nodes, providing essential insights into the complex structure of real-world systems. These networks consist of two mutually independent sets of nodes, where edges only occur between nodes in different clusters but not between nodes in the same cluster [11,12]. For example, let us consider a two-part network consisting of two separate types of nodes, a and b, and a two-part actor-movie network, where set a represents actors and set b represents movies. If actor i from node set a has acted in movie j from node set b, then there is a connection between nodes i and j in the two-part network, and there are no connections between the actors and movies in the two-part network. Although bipartite networks seem to be a type of network developed for a specific purpose, their use areas are widespread in many fields [13]. In recent years, bipartite networks have been applied in areas such as link prediction [14,15,16], social network analysis [17], and drug side effect prediction [18] [11].

With the popularization of bipartite networks in recent years, the link prediction studies in this area have also increased [19,20]. The first and natural attempt in this area is to convert bipartite networks into single-partite networks for discrete node types and then analyze them using the methods used in traditional single-partite networks. When these methods are examined, it is seen that the edge weights in single-partite networks obtained from bipartite networks are of particular importance. An edge weight in reflected networks is the closeness between the nodes forming this edge. Developing new link prediction approaches that can be applied directly to bipartite networks is an essential step toward a better understanding these structures.

2. Complex Networks

Networks are widely used to represent various real-world systems, such as social, biological, and technological information systems in nature and society. In these networks, vertices represent entities, and edges represent relationships or

interactions between vertices. A complex network is a type of realistic network constructed from real-world data. It has topological properties usually seen in accurate graphs but more trivial than in simple networks such as random graphs [21,22,23] or grid lines. Most real-world networks are complex networks. In particular, social networks, which model social structures such as friendship, kinship, co-authorship, and shared interests among people, are a type of complex network. Complex networks and their properties have attracted the attention of researchers in various fields. A complex network can be any real-world network with an abstract form without a predefined structure or evolutionary pattern. They can be highly dynamic, constantly changing or evolving. Moreover, in this era of big data, networks that start with a small form can grow to a staggering size quickly. This problem is significant for network scientists who want to analyze dynamic large-scale networks.

3. Analysis of Complex Networks

The analysis of complex networks, traditionally known as Social Network Analysis (SNA), examines the relationships and flows between people, groups, organizations, computers, or other entities within network structures through various techniques and deriving meaningful results from the obtained data. Social network analysis was previously used more intensively in social and behavioral sciences, but today, it is used in almost every field [1]. For example, social network analysis techniques, initially mainly used to examine individual and social group structures and behaviors, are now applied in more complex fields such as economics, education, trade, health, and banking.

Graph theory has emerged as an essential tool for analyzing complex networks. Its roots are mostly in sociology and mathematics, but it has rapidly gained importance in network analysis in biology, physics, telecommunications, computer science, etc. Graph theory has various sections of analysis, such as structural analysis of the network, temporal analysis that studies the evolution of networks, content-based analysis, etc.

The study of networks dates back to the pioneering work in mathematical graph theory by the Swiss mathematician Leonhard Euler, who solved the Königsberg Bridge problem (a circular journey that would pass exactly once across each of the Prussian bridges of Königsberg) in 1736. Euler attempted to solve the problem with graphs, as shown in Figure 2.3. In the 1950s and 1960s, random networks (graphs simulated by some simple random processes) were studied by Rapoport [24] and Erdos and Renyi [25,26]. In recent years, the development of

modern computers and the Internet has made it possible and convenient to capture, store, and analyze complex real-world networks, such as large-scale social networks, neuronal networks, and computer networks. Many interesting common properties and patterns have been discovered in real networks that differ significantly from random networks. Some examples of common network properties presented in many real networks include small-world economies [27], power-law degree distribution, community structures, auxiliary mixing, and many kinetic properties exhibited in the growth process of social networks. These insights have incredibly advanced people's understanding of complex systems in our world and inspired major works by people in complex network analysis [28].

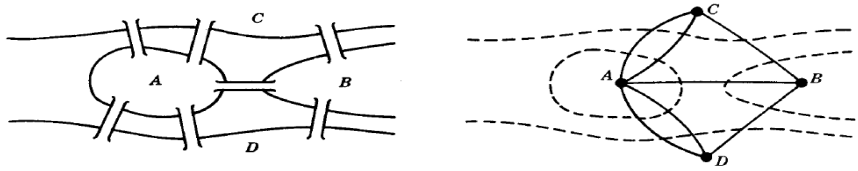


Figure 1. Königsberg's two islands and seven bridges

Nowadays, complex network analysis has attracted the attention of scientists from many disciplines, such as anthropology, sociology, biology, physical economics, geography, and information sciences. Current research interests mainly include

- the application of advanced concepts and measurements to accurate data and situations,
- the description of network structure,
- the observation of the characteristic structure of the network, and
- the development of new concepts and measurements to analyze the related elements.

It also includes studying network structure and function, analyzing network topology and evolutionary development, and applying social network analysis [29].

The analysis of social networks is done with three elements: actor, relationship, and tie. Actors are the essential elements of a social network and are shown with nodes. The relationships of all nodes are shown in a diagram. The corners

and edges of this diagram show the actors and relationships, respectively. Relationships are divided into content, direction, intensity, and active/passive relationships. The content shows the relationship between the two actors. Direction is classified as directional and non-directional. Intensity is expressed in time. An example is a two-year-long relationship between students studying at a school. Active and passive relationships show the type of relationship. The ties important for analyzing social networks are divided into strong and weak groups. Strong relationships are close, unique, and active. Weak relationships contain few relationships or communication information [30].

3.1. Graph Theory

Simple graphs are undirected, parallelogram-free, and loop-free (no connection from a node to itself) and are created without weights. Edges have no direction and are symmetrical. They represent binary relationships between nodes.

Directed graphs are graphs in which the edges between nodes have a direction. A directed network or a directed graph is called a digraph.

Examples of directed networks include

- the Internet, which is run by redirecting from one page to another;
- the food web, the energy network from prey to predator, and
- the citation network, the network of citations from one publication to another.

Each edge is associated with an ordered pair of nodes.

Multi graphs are used when simple graphs are not sufficient. They are undirected, parallel-edged, and cycle-free graphs. Simple graphs are multiple graphs, but multigraphs are not simple graphs.

Weighted graphs [31] are graphs in which each edge is given a numerical value, a weight. Since the edge weight represents the strength of the connection between nodes, it is divided into two categories: strong and weak. In many cases, multigraphs are converted to weighted graphs, and the number of edges connecting two nodes is reflected in the edge weight.

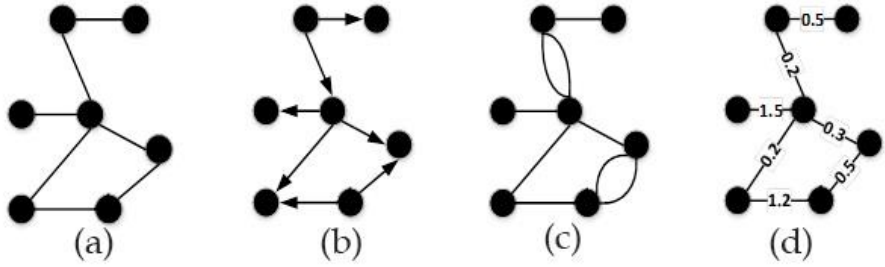


Figure 2. Graph models grouped according to the different types of edges found in a network (a. Simple graph, b. Directed graph, c. Multi graph, d. Weighted graph)

In directed networks, relationships can be one-way or two-way. For example, the relationship is one-way when one person follows or comments on Twitter. If the second person replies to or follows the first, the relationship becomes two-way. In network graphs, one-way relationships are shown with one-sided arrows, two-way relationships with two-sided arrows, and undirected relationships with lines without arrows. Another categorization of graphs can be made according to the type of connections between nodes. The graphs given in Figure 3 are examples of graph models categorized according to this property. The connection of a node in a graph is never formed with nodes in its cluster but only with nodes in different clusters. Alternatively, it can only be formed with nodes in its cluster.

3.2. Graph Types

Unipartite graphs: A type of graph in which no nodes are partitioned. There is only one set of nodes, and each node can be connected to another. For example, a co-authorship or scientific collaboration network is a monopartite network.

Bipartite graphs: A bipartite graph has two sets of nodes, and edges only occur between different sets of nodes. There are no connections between nodes in the same set of nodes. For example, Author-article academic knowledge networks consisting of authors and their scientific articles are bipartite. Another example is a student-course network consisting of one side of the students and the other set of nodes representing their courses, which is also a bipartite network. In these networks, connections only occur between authors and scientific article publications. Bipartite networks can be converted into single-partite networks. For example, the author-article bipartite network can be decomposed into two single-partite networks consisting of only authors and the other consisting of only scientific articles. When creating a single-partite author-author network, authors with at least one standard article in the bipartite network are connected. Similarly, when creating a single-partite article-article network, articles are connected if

they have at least one familiar author in the bipartite network. The single-partite graph model is a beneficial method. However, converting binary networks to single-partition networks causes much information about the network to be ignored. For example, when the author-article network is converted to a single-partition network, the information about which authors contributed to which article is available in the two-partition network. However, this information is not available in the single-partition author-author network.

Tripartite graphs: This type of graph consists of three sets of nodes in a similar manner.

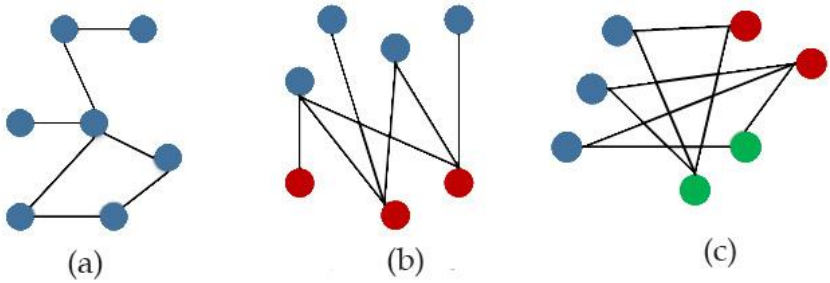


Figure 3. Different types of graphs (a. Unipartite, b. Bipartite, c. Tripartite)

4. Link Prediction

Social networks are complex information networks consisting of actors and relationships between actors. These networks show the interaction and cooperation between the same or different types of people or other multitudes. While the elements or entities in social networks constitute nodes, the interactions between nodes represent connections. Social networks have a very complex and dynamic structure by nature. New connections and entities appear or disappear over time in the network. This makes them dynamic and complex systems to a great extent. Connection prediction is an effective mathematical tool to analyze the uncertainty and potential relationship between non-neighboring nodes in complex networks [32]. Connection prediction is an effective social network analysis tool that focuses on the connections between two nodes from the changes in the social network. It is difficult to predict whether new relationships will form or existing ones will disappear from social networks. In parallel with the social network structure, it is also necessary to choose the quality to be estimated on this network correctly. This is also a significant problem. In the information age society we live in, thanks to the relationships in these networks, we can examine the social behaviors

of individuals, make qualitative and quantitative evaluations about human relationships, and obtain beneficial information from them [33].

Link prediction reveals possible relationships that are difficult to understand directly or predict future behavior [34]. Link prediction methods have attracted the attention of many researchers in different disciplines, such as social, biological, and information systems. Today, link prediction structure is used in the bibliographic field [3], molecular biology, forensic investigations, recommendation systems, medicine, etc. This process is used for different purposes in many studies. In social networks, in the future, which nodes may have new relationships or which existing relationships may be lost, which groups are in the network depending on the density of the relationships between nodes, which nodes are in which groups, which nodes affect other nodes more, etc. answers to questions are being investigated. In recent years, studies in this field have shown a significant increase. Link prediction can be applied in many necessary fields. Large organizations can be advised on potential collaborations, academic writers can be advised on authors or topics they can work on, criminal activities can be predicted by examining the relationships of criminals on social media or in phone calls, link prediction can be made on websites, the most suitable products can be recommended according to the behavior of users in e-commerce, protein-protein, disease-gene, disease-drug interactions can be predicted in bioinformatics, and the missing part of any incomplete social network data can be predicted.

4.1. Link Prediction Problem

The problem of predicting new connections (or simply the link prediction problem) is to make predictions about the structure of the connections in the network by examining the history of the emergence and disappearance of connections in the network over a certain period. The link prediction problem, one of the most critical research areas of social network analysis, is classically defined as follows: “Connection prediction is the process of correctly predicting the edges that will be added to the network from time interval t to a certain future time, given the current state of a social network at time t.” [7].

To describe it mathematically, let us consider the social network G=(V, E) at a given time t, where V represents the node-set and E represents the connection set, respectively. Connection prediction aims to predict the lost or newly formed connections between nodes or the missing or unobserved connections in the current network for the future t' ($t' > t$). Let us explain the connection prediction problem with the social network represented by

the friendship relations of five people given in Figure 4. Here, the solid and solid lines show the existing interactions at time t, while the solid lines show the newly emerged interactions in the time interval [t, t′]. At times, Adam and Maria are friends, and Maria is also with Sophia. Perhaps at time t′, Maria introduced Adam to Sophia, and thus they became friends. Similarly, David and Sophia become friends at time t′. Here, the connection prediction problem aims to predict the new friendship relations that will be formed between people.

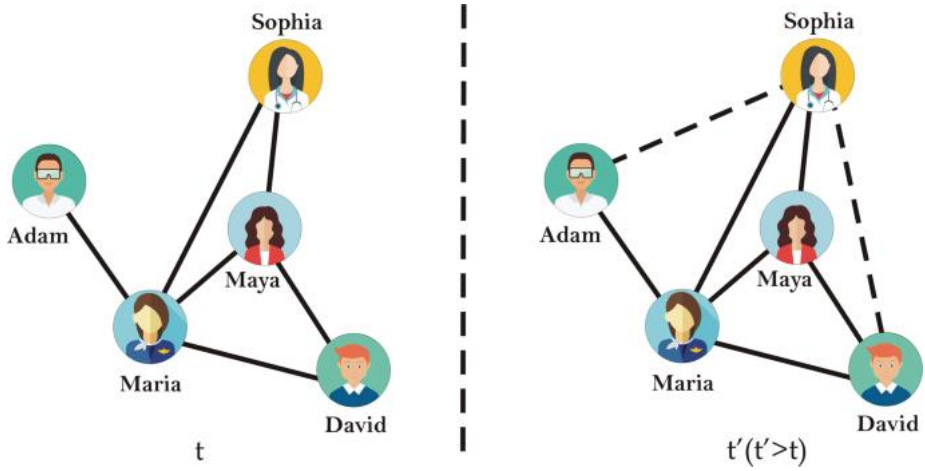


Figure 4. An example to illustrate the link prediction problem

4.2. Link Prediction Techniques

The problem of link prediction in social networks is a long-standing problem in modern information science [35]. The computer science community proposed probabilistic models based on Markov chains and statistical models [36]. Later, models based on network structure, such as the subgraph-based ranking model [37] and the local information model [38], were used. As good results were obtained from studies based on network structure and node attributes, studies were conducted with local conditional probability models that used both methods. Link prediction approaches using topological approaches can be classified as structural and temporal, depending on whether the network's evolutionary development is considered or not. Figure 5 shows two types of link prediction.

Structural link prediction refers to the problem of finding missing or hidden connections in an existing network [7]. It aims to reveal connections in the network that cannot be directly seen using existing data. It has a direct

applicability feature to find protein interactions and gene patterns that cannot be seen in medical studies on various diseases such as cancer, HIV, Alzheimer's, etc. [39]. In addition, criminal actions that may occur can be predicted by examining the relationships of criminals on social media or in phone calls.

Time-dependent link prediction refers to the problem of finding connections that will occur in the next period by examining the temporal history of a network [4,7]. In this link prediction method, we have information about the network observed until time t, and we aim to predict new connections that may occur at the next time, such as t+k. For example, products that customers can buy in their next shopping can be suggested on e-commerce shopping sites, and they can be used for friend recommendations on many social media sites such as Facebook, Twitter, and Flickr. In academic knowledge networks, it can be predicted with which academics will collaborate in the future [21].

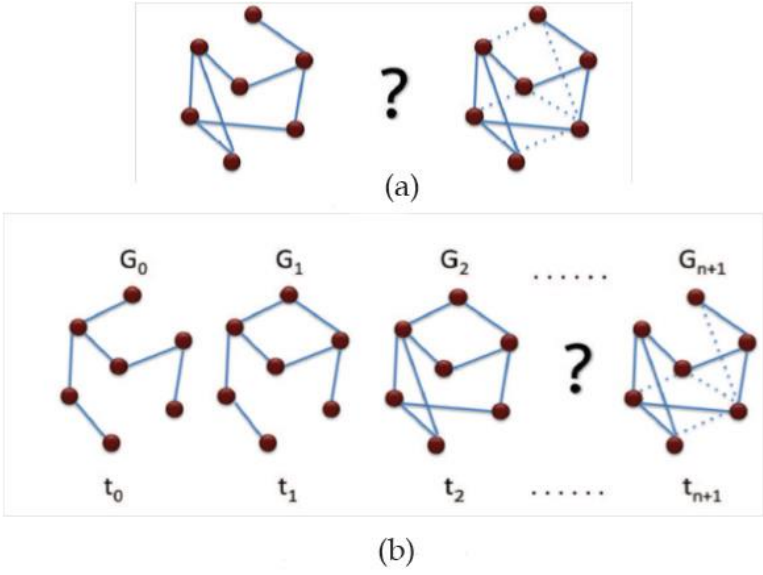


Figure 5. Types of structural and temporal link estimation using topological properties of the network (a. Structural link estimation, b. Temporal link estimation)

In the link prediction problem, if nodes are considered as V (data samples), $V = \{v_i\}_{i=1}^{n}$, and E represents the relationships that exist on this data. Accordingly, a social network can be defined by the graph $= (V, E)$. Here, there will be (vi, vj) node pairs. Between these node pairs, $e_{ij} \notin E$ is tried to estimate the unformed link. The criterion showing the importance of the link between node pairs can be defined as the $skor(x, y)$ function. In the literature, the metrics commonly used for link prediction in social networks can be categorized as semantic

or topological-based metrics. For example, in the author collaboration network, future interactions between authors can be predicted by the similarity in the keywords of the articles [8].

In semantic metrics, the nodes' content is considered when calculating the similarity between nodes. For example, in the co-authorship network, the ethnic origins of the authors, their educational background, and the similarity between the topics they have worked on during their academic careers can be used to estimate the link. The information required for semantic metrics may often be outside the network or costly to analyze. Topological metrics are more commonly used because they are more general and do not require a rich description of content-related features [28]. Some approaches use both semantic and topological features. These approaches can also be called hybrid approaches. Many link prediction metrics use topological features such as nodes, topological structure, and social theory information to calculate the similarity of pairs of nodes in the network. Learning-based link prediction metrics are also more complex than these three categories. Learning-based metrics use both topological and semantic features.

Node-Based Metrics

When considering the problem of link prediction, the most intuitive solution that can be considered is to calculate the similarity ratio between given node (actor) pairs. The probability of a link between two nodes with no link is directly proportional to the similarity between the nodes. In this study, the numerical value indicating the similarity between a pair of nodes x and y that have no link in the current network is represented by $skor(x,y)$. A high score represents a high probability that nodes x and y will be connected in the future, while a low score indicates that they will not. By using the order of the calculated similarity scores from largest to smallest, it is possible to predict the connections that will be formed or lost in the future or those that are not visible in the current network.

In a classical social network consisting of nodes and relationships between nodes, nodes can have various properties. For example, in social media applications (Facebook et al., etc.), users usually have properties such as career, address, religion, and interests. These properties can be directly used to calculate the similarity between two nodes. In most cases, the attribute values of nodes are kept in text or string format. As a result, node-based metrics are mainly based on attributes and actions that can reflect nodes' personal characteristics and behaviors. Therefore, node-based metrics are helpful in link prediction only in cases where such information is easily obtained.

Topology Based Metrics

As mentioned, similarity measures are divided into semantic and topological features. Finding semantic features in node-based measures where node features are used is challenging. The topological-based measures presented in this section use the network's topological (structural) information rather than the node and edge information. In the last decade, many topological-based measures have been proposed to calculate the similarity of two nodes in a simple network where node and edge features are absent. Topological measures are generally categorized in the literature under three headings: neighborhood-based, path-based, and random walk-based. This section will give a general definition of some of the most popular measures in these categories. For a better understanding of the definitions, some standard symbols used in link prediction methods are given in Table 1.

Table 1. Common symbols used in link prediction metrics.

$\Gamma(x)$	set of neighbors of x
$\Gamma(y)$	set of neighbors of y
$\|\Gamma(x)\|$	Number/degree of neighbors of node x
$\|\Gamma(y)\|$	Number/degree of neighbors of node y

Neighborhood-Based Measures

In social networks built from real-world data, nodes tend to form new connections with nodes that are similar to them. In neighborhood-based metrics, the similarity ratio is calculated using the common neighbors of the node pair. The basic idea is that the more the neighbors Γ(x) and Γ(y) of nodes x and y overlap, the higher the probability of a connection between them in the future. There are many neighborhood-based metrics proposed in this field.

Common Neighbors (CN), The familiar neighbors criterion shows the number of common neighbors for nodes x and y. Due to its simplicity has become the most common criterion used in link prediction problems. Many different criteria have been derived using familiar neighbors. The higher the number of common neighbors, the higher the probability of a link between nodes x and y in the future. The mathematical equivalent of this expression is as shown in equation (1).

$$CN(x,y) = |\Gamma(x) \cap \Gamma(\mathrm{y})| \quad \textbf{(1)}$$

Jaccard Coefficient (JK) is the normalized form of the familiar neighbors [35]. It calculates the ratio of the familiar neighbors of nodes x and y to the total number of all their neighbors. Node pairs with a higher ratio have more similarity. The mathematical equivalent of this expression is as shown in equation (2).

$$JK(x,y) = \frac{|\Gamma(x) \cap \Gamma(y)|}{|\Gamma(x) \cup \Gamma(y)|} \quad \textbf{(2)}$$

Adamic/Adar Coefficient (AA) *was first proposed by Adamic and Adar [40] to calculate how close the content of two web pages is to each other. It has later been widely used in social networks. Unlike the familiar neighbors (CN) metric, this metric argues that the weight of familiar neighbors with fewer neighbors will be higher. The mathematical equivalent of this expression is as shown in equation (3).*

$$AA(x,y) = \sum_{z \in \Gamma(x) \cap \Gamma(y)} \frac{1}{\log|\Gamma(z)|} \quad \textbf{(3)}$$

Cosine Similarity Coefficient (Cos) is also called Salton Cosine similarity [38], is used to find the similarity coefficient based on the cosine angle between the rows of the adjacency matrix with nodes x and y. The mathematical equivalent of this expression is as shown in equation (4).

$$Cos(x,y) = \frac{|\Gamma(x) \cap \Gamma(y)|}{\sqrt{|\Gamma(x)|.|\Gamma(y)|}} \quad \textbf{(4)}$$

Social Theory Based Measures

Many studies have been conducted in recent years to solve social network mining and analysis problems. Most of the studies in this field use classical social theories such as community, weak and robust connection concepts, homogeneity, and structural balance. Unlike previous measures that use only node and topological features, link prediction measures based on social theory can increase prediction performance by revealing useful social interaction information, especially for large-scale social networks.

Learning Based Measures

Learning-based link prediction metrics are based on both node-based and topology-based features. In recent years, many learning-based link prediction methods have been proposed using the attributes and external information of nodes [26]. These learning-based methods can be categorized as feature-based classification, probabilistic graph model, and matrix factorization. Most learning-based methods can be considered a typical feature classification problem. Scellato et al. [6] used social features such as spatial information and global features to improve the quality of link prediction in a location-based social network. In social networks, a probability value such as topological similarity or transition probability in a random walk can be assigned to the link between each pair of nodes. The

graphs generated by this method are called probabilistic graph models. Many learning-based link prediction methods in the literature are based on probabilistic graph models.

5. Conclusions

Link prediction in complex networks is a critical research area for predicting missing or potential links in various social, biological, and technological systems. The methods used in this study are enriched with topological features, machine learning algorithms, and deep learning techniques, and successful results have been obtained for different types of networks. In particular, classical approaches based on similarity measurements between nodes provide accuracy and computational efficiency advantages. In contrast, advanced methods such as graph neural networks have provided more accurate predictions in large and dynamic networks. In the future, improving data quality and examining heterogeneous networks in more depth will further improve link prediction performance and increase the impact of this field on applications such as social network analysis, bioinformatics, and information recommendation systems.

REFERENCES

[1] Wasserman, Stanley. "Social network analysis: Methods and applications." *The Press Syndicate of the University of Cambridge* (1994).

[2] Tang, Feiyi. *Link-prediction and its application in online social networks*. Diss. Victoria University, 2017.

[3] Hwang, San-Yih, Chih-Ping Wei, and Yi-Fan Liao. "Coauthorship networks and academic literature recommendation." Electronic Commerce Research and Applications 9.4 (2010): 323-334.

[4] Al Hasan, Mohammad, et al. "Link prediction using supervised learning." SDM06: workshop on link analysis, counter-terrorism and security. Vol. 30. 2006.

[5] Folino, Francesco, and Clara Pizzuti. "A comorbidity-based recommendation engine for disease prediction." 2010 IEEE 23rd International Symposium on Computer-Based Medical Systems (CBMS). IEEE, 2010.

[6] Scellato, Salvatore, Anastasios Noulas, and Cecilia Mascolo. "Exploiting place features in link prediction on location-based social networks." Proceedings of the 17th ACM SIGKDD international conference on Knowledge discovery and data mining. 2011.

[7] Liben-Nowell, David, and Jon Kleinberg. "The link prediction problem for social networks." Proceedings of the twelfth international conference on Information and knowledge management. 2003.

[8] Xiang, Evan Wei. "A survey on link prediction models for social network data." Science and Technology (2008).

[9] Hasan, Mohammad Al, and Mohammed J. Zaki. "A survey of link prediction in social networks." Social network data analytics (2011): 243-275.

[10] Katz, Leo. "A new status index derived from sociometric analysis." Psychometrika 18.1 (1953): 39-43.

[11] Gao, Man, et al. "Projection-based link prediction in a bipartite network." Information Sciences 376 (2017): 158-171.

[12] Latapy, Matthieu, Clémence Magnien, and Nathalie Del Vecchio. "Basic notions for the analysis of large two-mode networks." Social networks 30.1 (2008): 31-48.

[13] Latapy, Matthieu, Clémence Magnien, and Nathalie Del Vecchio. "Basic notions for the analysis of large two-mode networks." Social networks 30.1 (2008): 31-48.

[14] Chang, Yang-Jui, and Hung-Yu Kao. "Link prediction in a bipartite network using Wikipedia revision information." 2012 Conference on Technologies and Applications of Artificial Intelligence. IEEE, 2012.

[15] Nigam, Aastha, and Nitesh V. Chawla. "Link prediction in a semi-bipartite network for recommendation." Intelligent Information and Database Systems: 8th Asian Conference, ACIIDS 2016, Da Nang, Vietnam, March 14–16, 2016, Proceedings, Part II 8. Springer Berlin Heidelberg, 2016.

[16] Wang, X., Liu, Y., & Xiong, F. (2016). Improved personalized recommendation based on a similarity network. Physica A: Statistical Mechanics and its Applications, 456, 271-280.

[17] De Sá, H. R., & Prudêncio, R. B. (2011, July). Supervised link prediction in weighted networks. In The 2011 international joint conference on neural networks (pp. 2281-2288). IEEE.

[18] Luo, Yifu, et al. "Predicting drug side effects based on link prediction in bipartite network." 2014 7th International Conference on Biomedical Engineering and Informatics. IEEE, 2014.

[19] Li, Xin, and Hsinchun Chen. "Recommendation as link prediction in bipartite graphs: A graph kernel-based machine learning approach." Decision Support Systems 54.2 (2013): 880-890.

[20] Xia, Shuang, et al. "Link prediction for bipartite social networks: The role of structural holes." 2012 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining. IEEE, 2012.

[21] Newman, Mark EJ. "The structure of scientific collaboration networks." Proceedings of the national academy of sciences 98.2 (2001): 404-409.

[22] Bollobás, B. "Random Graphs 2001 2 Cambridge Cambridge University Press 10.1017." CBO9780511814068 Google Scholar Google Scholar Cross Ref Cross Ref.

[23] Breiman, Leo. "Random forests." Machine learning 45 (2001): 5-32.

[24] Rapoport, Anatol, and Lionel I. Rebhun. "On the mathematical theory of rumor spread." The bulletin of mathematical biophysics 14 (1952): 375-383.

[25] ERDdS, P., and A. R&wi. "On random graphs I." Publ. math. debrecen 6.290-297 (1959): 18.

[26] Erdos, Paul. "On the evolution of random graphs." Bulletin of the Institute of International Statistics 38 (1961): 343-347.

[27] Cavanagh, Allison. "Imagining networks: The sociology of connection in the digital age." Digital Sociology: Critical Perspectives. London: Palgrave Macmillan UK, 2013. 169-185.

[28] Allali, Oussama, Clémence Magnien, and Matthieu Latapy. "Internal link prediction: A new approach for predicting links in bipartite graphs." Intelligent Data Analysis 17.1 (2013): 5-25.

[29] Goldenberg, Anna, et al. "A survey of statistical network models." Foundations and Trends® in Machine Learning 2.2 (2010): 129-233.

[30] Chang, Wei-Lun, and Tzu-Hsiang Lin. "A cluster-based approach for automatic social network construction." 2010 IEEE Second International Conference on Social Computing. IEEE, 2010.

[31] Newman, Mark EJ, and Michelle Girvan. "Finding and evaluating community structure in networks." Physical review E 69.2 (2004): 026113.

[32] Allali, Oussama, Clémence Magnien, and Matthieu Latapy. "Internal link prediction: A new approach for predicting links in bipartite graphs." Intelligent Data Analysis 17.1 (2013): 5-25.

[33] Goldenberg, Anna, et al. "A survey of statistical network models." Foundations and Trends® in Machine Learning 2.2 (2010): 129-233.

[34] Chang, Wei-Lun, and Tzu-Hsiang Lin. "A cluster-based approach for automatic social network construction." 2010 IEEE Second International Conference on Social Computing. IEEE, 2010.

[35] Newman, Mark EJ, and Michelle Girvan. "Finding and evaluating community structure in networks." Physical review E 69.2 (2004): 026113.

[36] Zhu, Jianhan, Jun Hong, and John G. Hughes. "Using markov chains for link prediction in adaptive web sites." Int. Conference on Soft Issues in the Design, Development, and Operation of Computing Systems. Berlin, Heidelberg: Springer Berlin Heidelberg, 2002.

[37] Guo, Fangjian, Zimo Yang, and Tao Zhou. "Predicting link directions via a recursive subgraph-based ranking." Physica A: Statistical Mechanics and its Applications 392.16 (2013): 3402-3408.

[38] Zhou, Tao, Linyuan Lü, and Yi-Cheng Zhang. "Predicting missing links via local information." The European Physical Journal B 71 (2009): 623-630.

[39] Airoldi, Edo M., et al. "Mixed membership stochastic blockmodels." Advances in neural information processing systems 21 (2008).

[40] Adamic, Lada A., and Eytan Adar. "Friends and neighbors on the web." Social networks 25.3 (2003): 211-230.

CHAPTER 3

Use of Deep Learning in Medical Imaging

Gül Cihan Habek[1] & Fatih Başçiftçi[2]

[1] Res. Asc., Karamanoglu Mehmetbey University, Orcid: 0000-0003-1748-3486
[2] Prof. Doct., Selcuk University, Orcid: 0000-0003-1679-7416

1. Introduction

Deep learning, a sub-branch of artificial intelligence and machine learning, was developed by taking inspiration from the working principle of the human brain (Guo, 2017). Deep learning algorithms show higher performance than traditional machine learning algorithms in solving complex problems thanks to their ability to work with very large data sets. Deep learning models are frequently used in a number of tasks such as disease diagnosis and classification, object detection, face recognition, emotion analysis, and road condition prediction (Khoei, Slimane, & Kaabouch, 2023).

Medicine is a branch of science that deals with the structure and functioning of the human body and produces very important information about human health by performing various analyses in cases such as diseases and injuries. Various medical imaging techniques are used to examine the biological and medical processes of the human body and to perform the necessary analyses. The foundation of these imaging techniques was laid in the 19th century by German Physics Professor Wilhelm Conrad Röntgen with the discovery of X-rays, which allowed the imaging of bones and internal organs in the body (Mould, 1995). Shortly after the discovery of X-rays, natural radioactivity was discovered by French scientist Henri Becquerel in the same (Samei & Peck, 2019). Immediately after Becquerel's discovery, the elements polonium and radium were discovered by Polish scientist Marie Curie and her husband, who were working in France. Thanks to these discoveries, the science of radiology emerged; the technologies and imaging techniques used in radiology formed the basis of the field of medical imaging (Man, Sabourin, Gandhi, Carmel, & Prestigiacomo, 2015).

Advanced medical imaging techniques such as Magnetic Resonance Imaging, Computerized Tomography, Positron Emission Tomography, and Ultrasonography used today; allow for accurate and timely diagnosis of diseases. With the advancement of technology and science, high-resolution and high-quality images have begun to be obtained from medical imaging techniques in recent years. The number of images taken is increasing day by day and forms large data sets related to diseases. This situation has led to the idea of using deep learning algorithms, which show good performance when working with large data sets, in the process of interpreting medical images.

Medical Image Processing is a field performed by computers to analyze and interpret images obtained from biomedical imaging techniques (Khoei et al., 2023). Recently, Medical Image Processing has become an important application

area of deep learning. Deep learning algorithms are used in the analysis of appropriate medical images taken from various regions such as the brain, eye, skin, teeth, chest, breast, heart, abdomen, and musculoskeletal system, and provide faster, more precise and objective results than human interpretations in the diagnosis and classification of various diseases such as Alzheimer's, brain hemorrhage lesions, diabetic retinopathy, dental diseases, lung cancer, breast cancer, liver tumors and skin lesions (Greenspan, Van Ginneken, & Summers, 2016; Litjens et al., 2017).

When the studies in the literature on the use of deep learning in the medical field are examined, in one of the studies Togo et al. (2019) proposed the deep GAN-based LC-PGGAN model to produce synthetic examples of gastritis images diagnosed with stomach X-ray images that can be used in the gastritis classification problem. New synthetic data sets were created using LC-PGGAN, LC-PGGAN+PGGAN, PGGAN, and DCGAN architectures from stomach X-ray images of 240 gastritis and 575 non-gastritis patients. When the real data set and synthetic data sets were classified using VGG-16, Inception-v3, and ResNet-50 deep learning architectures, the best result in the VGG-16 architecture was obtained when the data set produced with LC-PGGAN was used, and the best result for Inception-v3 and ResNet-50 architectures was obtained with the data set created by using LC-PGGAN and PGGAN together.

Jiajie (2020) aimed to extract features from brain computed tomography (CT) images using deep convolutional neural networks and classify them according to 5 subcategories of intracranial hemorrhage. The dataset used in the study consists of images provided by the North American Radiology Association through a competition organized on the Kaggle platform. The model, which was created using a series of deep convolutional neural networks based on SE-ResNeXt50 and EfficientNet-B3, achieved high performance in the classification study and managed to enter the 4% segment in the competition.

Sarp et al. (2021) proposed a new generative adversarial network model based on GAN architecture to generate synthetic wound images. The performance of the model trained on chronic wound datasets of various sizes taken from real hospital environments was evaluated using mean square error (MSE) to measure the similarity of the original and synthetic images. At the end of the study, it was concluded that the proposed synthetic medical image generation model showed good performance.

In another study, Mushtaq et al. (2021) conducted a study on the classification of brain hemorrhage using deep learning-based CNN and CNN+LSTM and

CNN+GRU hybrid-based models proposed in the study. The main purpose of the study is to enable the deep learning model to grasp patterns and derive rules and features from them in cases where the number of data is insufficient. For this purpose, a brain hemorrhage dataset consisting of a small number of images was created using 100 hemorrhagic and non-hemorrhagic CT images taken from patients. Image augmentation techniques were used to increase the diversity of the dataset. A new architecture called BHCNet was proposed by using image augmentation and dataset imbalance methods together with the CNN model.

Siddiqui et al. (2021) proposed a cloud-based model called IPBCS-DL, powered by deep learning, to predict breast cancer and its stages. In the study, a dataset consisting of images obtained from various tests such as CT, magnetic resonance imaging (MRI), and positron emission tomography (PET) was used, and the proposed model showed a higher performance than the current state-of-the-art methods with 98.86% accuracy in the training phase.

Ayala et al. (2021) aimed to make an early diagnosis of Diabetic Retinopathy (DR) and determine its degree using a model based on the DenseNet121 transfer deep learning architecture. In the study where two different data sets were used, the images were divided into five different classes according to the presence and degree of the disease: DR-no, mild-DR, moderate-DR, severe-DR, and proliferative-DR. The proposed model showed a classification performance of 97.78%, allowing diabetic retinopathy to be predicted reliably.

Bangyal et al. (2022) proposed a deep convolutional neural network model for early detection of Alzheimer's disease. In the study, the Alzheimer's dataset consisting of four classes, namely very mildly demented, mildly mentally retarded, moderately retarded, and non-demented, shared on the Kaggle platform, was used. When the results obtained from machine learning-based approaches and the proposed deep learning-based convolutional neural network approach were compared, the proposed approach showed the best performance with 94.61% accuracy.

In the next study, Ren et al. (2022) proposed a new hybrid architecture called LCGANT for the classification of lung cancer. The proposed architecture consists of two parts: the lung cancer deep convolutional GAN (LCGAN) developed to create a synthetic lung cancer image and the VGG-DF transfer learning model used to classify the images. In the study, where a dataset consisting of a total of 15000 lung images belonging to three different classes was used, the LCGANT model gave the best result with 99.84% classification accuracy compared to the other models used.

Hoang et al. (2022) conducted a study on the classification of skin lesions. In the study, a new EW-FCM segmentation approach was developed and a new method called Wi-de-ShuffleNet was proposed for classification. In the study, where two different data sets, HAM10000 and ISIC 2019, available on the Kaggle platform, were used, it was concluded that the proposed method achieved higher accuracy compared to recent approaches.

In another study on skin diseases, Anand et al. (2022) used dermoscopy images to perform early diagnosis and classification of skin diseases. The HAM10000 dataset, which consists of images related to seven different skin diseases, was used in the study and a new deep-learning model was developed for the classification of skin diseases. When the accuracy values obtained with ResNet18, ResNet50, ResNet101, and the model proposed in the study were compared, the proposed model showed the highest performance with 96%.

Jyotiyana et al. (2022) tried to diagnose and classify Parkinson's disease using deep learning methods. In the study, a Parkinson's dataset consisting of voice recordings and some information of 42 patients in the early stages of the disease was used and 42 patients were recruited for a 6-month trial on a remote monitoring device to follow the progression of the disease. A new deep learning model has been proposed for the classification of the disease, and the proposed model gave a better accuracy value than other classification techniques with a classification accuracy of 94.87%.

In the study conducted by Qureshi et al. (2022), a deep learning model called DLM-COVID-19, which extracts MR neuroimaging findings in severe COVID-19 infections, was proposed for the detection and classification of COVID-19 disease. The COVID-19 dataset required for the study was created by collecting MR images of approximately 50 individuals who had the disease from various hospitals with the help of medical experts. It was concluded that the proposed model gave better results compared to existing methods in the study. In addition, a mobile detection system was developed that allows the patient to visit the online system, ask questions, and produce results about their health status.

Torfi et al. (2022) tried to produce synthetic medical data by developing a convolutional GAN model to overcome the privacy problem of medical images. Since synthetically generated data does not contain sensitive information about the person, it can be shared with the public without privacy concerns, thus increasing the workability of deep learning models working with large data sets with medical images. The RDP-CGAN architecture proposed in the study using Rényi differential privacy produced higher quality synthetic data under the same

privacy when applied to different data sets compared to the current most advanced approaches, MedGAN, TableGAN, CorGAN, DPGAN, and PATE-GAN.

Pravin et al. (2023) proposed a new model based on DenseNet, which includes an automatic preprocessing module for the determination of the severity level of diabetic retinopathy. The model, which was trained on a dataset consisting of 13000 retinal fundus images taken from the diabetic retinopathy database, achieved a classification accuracy performance of 98.40% when combined with the k-nearest neighbor classifier.

Abdulsahib et al. (2023) conducted a study on the classification of liver cancer with deep transfer learning methods. In the study, a dataset related to the disease in question was created by collecting CT images from the Institute of Radiology in Baghdad Medical City, Iraq. To classify the images in the obtained dataset as a malignant tumor, benign tumor, or normal liver, some layers of ResNet-50, VGG-16, and MobileNetV2 transfer learning methods were frozen and it was aimed to increase the performance by using new fully connected layers with random parameters instead of the layers from the pre-trained models. In the study where the effectiveness of the three transfer learning approaches was evaluated, the ResNet-50 model showed the highest performance with 100% accuracy.

Naz et al. (2023) conducted a study on solving the problem of data scarcity and irregular data distribution in diabetic retinopathy. In the study, the Deep Convolutional Generative Adversarial Network (DCGAN) algorithm was used to combine real and augmented views, and the data imbalance problem was tried to be resolved by including the generated images in the minority class. In the study, a new ensemble convolutional neural network algorithm called DVE, which combines the weighted average estimate of CNN, CNN-i, and CNN+i algorithms, was proposed, and 97.4% classification accuracy was achieved on the balanced data set with DCGAN.

Tabakov et al. (2023) addressed the problem of incomplete data sets in their study and developed a new synthetic data generation model to increase the number of histopathology image data. In this direction, experiments were carried out using the Shiraz Histopathological Imaging Data Center dataset. When ResNet-18, DenseNet, EfficientNet, GoogLeNet, MobileNetV2, and VGG-11 deep learning models were trained with the synthetic data produced in the study and the f1 score values were compared, the best result was obtained with the EfficientNet model as 88%.

Oliveira et al. (2024) tried to produce synthetic data from retinal fundus images to cope with the small dataset problem in medical images. The datasets used

in the study included publicly available retinal fundus images of patients from four different countries. The comparison of the proposed StyleGAN2-ADA model with nine different GAN architectures, namely DCGAN, LSGAN, WGAN, WGAN-GP, DRAGAN, EBGAN, BEGAN, CGAN and ACGAN; Whether experts can distinguish synthetic images as real or synthetic images; There are four experimental stages: evaluating the dataset augmented with synthetic images with three different deep transfer learning models, namely SqueezeNet, AlexNet and ResNet18, and measuring the recognition accuracy of AMD (Age-related Macular Degeneration) images of deep learning models trained with human experts and synthetic and real data. As a result of the experiments, it was concluded that the developed Style-GAN2-ADA model was successful in producing synthetic images.

Yang et al. (2024) proposed a new deep GAN model based on CycleGAN to generate synthetic computed tomography images from MR images. In the study, two different datasets consisting of unpaired brain MR and CT images shared on the Kaggle platform and paired brain MR and CT images taken from a study (Ranjan, Lalwani, & Misra, 2022; Wang, Wu, & Pourpanah, 2023) were used. With the proposed HLSNC-GAN model and eight different existing models, MR-to-CT and CT-to-MR transformations were performed for two datasets, and the best results were obtained with the HLSNC-GAN architecture in the results obtained with PSNR (Peak Signal-to-Noise Ratio) and SSIM (Structural Similarity Index Measure), which are widely used in the evaluation of medical image syntheses.

In the last literature study, Chen et al. (2024) proposed a new deep neural network model for the detection and classification of acute intracranial hemorrhages in brain CT images. Three datasets named RSNA, CQ500, and PhysioNet-ICH were created using images taken from different institutions and the RSNA dataset was used for training the proposed model. The proposed model achieved a successful classification by obtaining an average AUROC value of 0.942 and 0.958 in CQ500 and PhysioNet-ICH datasets, respectively.

In this study, VGG16, ResNet50, MobileNetV3Small, MobileNetV3Large, InceptionV3, and DenseNet201 deep transfer learning methods were used to classify two different diseases, Diabetic Retinopathy and Monkeypox. Different hyperparameter combinations were optimized with a genetic algorithm to increase the performance of transfer learning models. The models were trained with different hyperparameters and the final models were created by determining the hyperparameter combinations that provided the highest success. The performance of the created models was evaluated with accuracy, precision, recall, and f1-score

metrics, and the highest performance values were obtained for the two-class Diabetic Retinopathy dataset with DesNet201 architecture as 0.98 and for the four-class Monkeypox disease dataset as 0.93 for all four metrics.

In the continuation of the study, explanatory information about image processing, machine learning, and deep learning is given in Section 2; the datasets used in the study are explained and the deep transfer learning algorithms used are examined in detail. The results obtained from the study are explained in Section 3, and information about the results of the study and what is planned for future studies is given in Section 4.

2. Material and Method

In this section, the concepts of image processing, machine learning and deep learning are explained. In the following, explanatory information about the data sets used in the study is given and the deep transfer learning algorithms used are examined in detail.

2.1. Image Processing

Image is a concept that expresses the reflections of three-dimensional objects in real life on a two-dimensional plane. Images that can be processed and stored in a computer environment are represented by matrices consisting of pixels. Pixels are dots consisting of different intensities of the three primary color components (RGB), red, green and blue, and are the basic building blocks of digital images.

Image processing is the name given to the entire process of analyzing visual data of real-world objects represented in digital format using various techniques and changing the properties of these data (1991). Briefly, it is the transfer of the original input image from the analog environment to the digital environment and the analysis operations performed on the transferred image (Gonzalez, Woods, & Eddins, 2020). These operations are performed with the help of mathematical operations applied to the pixels that make up the image. Basically, image processing is performed in four steps as shown in Figure 1.

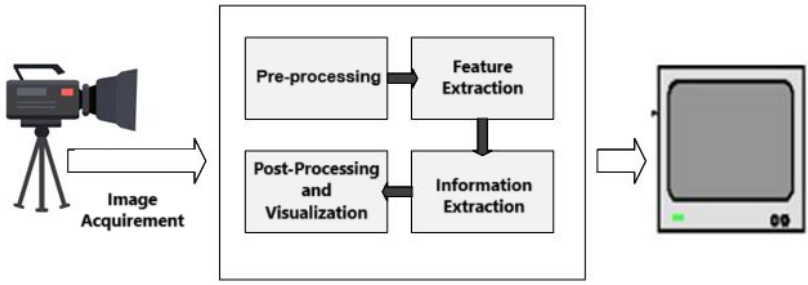


Figure 1. Basic steps in image processing

As shown in Figure 1, various pre-processing steps such as noise reduction, contrast adjustment, and size change are applied to the image obtained through digital cameras or sensors in the first stage to obtain a clean image. In the second stage, feature extraction algorithms are applied to the cleaned image to extract features that include visual elements such as edges, colors, and textures of objects. After the extraction of features, the information extraction step is performed using an algorithm designed to perform recognition, classification, or another task on the image depending on the field of study. The information obtained in the final processing stage is processed to be used in various disciplines such as medicine, security, and automotive. This information can be used in various applications, such as medical diagnoses, security systems, or automotive technologies.

To provide computer systems with complex visual information processing capabilities that mimic the visual functioning of living beings; machine learning and deep learning architectures are used in image processing applications (McAndrew, 2004). Machine learning and deep learning, especially when combined with the availability of large data sets, have gained the ability to solve larger and more complex problems compared to previous image processing methods. Today, deep learning-based image processing methods are used in a wide variety of fields such as medicine, security, automotive, agriculture, social media, and gaming, and successful results are obtained.

2.2. Machine Learning

The performance of some processes that require human intelligence, such as analysis, prediction and classification, by machines is called artificial intelligence (Choi, Coyner, Kalpathy-Cramer, Chiang, & Campbell, 2020). In other words, artificial intelligence means that computers imitate human intelligence and behave like them, thanks to models trained through various data sets and software.

Machine Learning, a sub-branch of artificial intelligence, is the study of computers being trained with past data and gaining the ability to make automatic decisions on a situation they have not encountered. While problems with clearly stated logical solutions are addressed with artificial intelligence, machine learning methods that show higher performance are used in problems that require high-level pattern recognition, such as classification of images, recommendation systems, autonomous systems, and natural language processing.

In cases where it is necessary to work with data that is too large and complex to be analyzed by human power, machine learning algorithms provide low-cost solutions in less time. Thanks to the rapid advances in computer science in recent years, machine learning algorithms used in different disciplines are also applied in the solution of various problems in the field of medicine and health, and they provide good results thanks to ongoing improvements. (Laurikkala et al., 2000).

2.3. Deep Learning

Deep learning is a sub-branch of machine learning that uses multiple layers designed to increase the performance of machine learning and to be used in more challenging tasks (LeCun, Bengio, & Hinton, 2015). This learning model, which takes its name from the deep neural networks it uses, allows machines to make correct decisions without any external intervention. Deep neural networks, which consist of two or more hidden layers, progress in an order established from simple to complex, with each layer trying to establish a relationship with the previous layer.

Deep learning, inspired by the working principles of the human brain, is used to solve complex problems by training on large amounts of data. It is used to solve various problems in different disciplines such as speech recognition, object detection, image processing, and natural language processing, and shows high performance compared to traditional machine learning algorithms (Ruihui & Xiaoqin, 2019).

2.4. Datasets

In the study, a classification study of two different diseases was conducted using the data sets “diagnosis-of-diabetic-retinopathy” (Darabi, 2024) and “monkeypox skin images dataset” (Bala et al., 2023) shared on Kaggle, an online platform for researchers working on machine learning and data science. Detailed explanations about the data sets used in the study are given under the following headings.

2.4.1. Dataset1: Diagnosis of Diabetic Retinopathy

The dataset consists of high-resolution retinal images obtained under different imaging conditions. Each image in the dataset was labeled as diabetic retinopathy present (DR) and absent (No_DR) by a medical expert, and examples of images in the dataset are shown in Figure 2. In addition, the classes in the dataset are distributed evenly, and the number of data in the classes and the total number of data are given in Table 1.

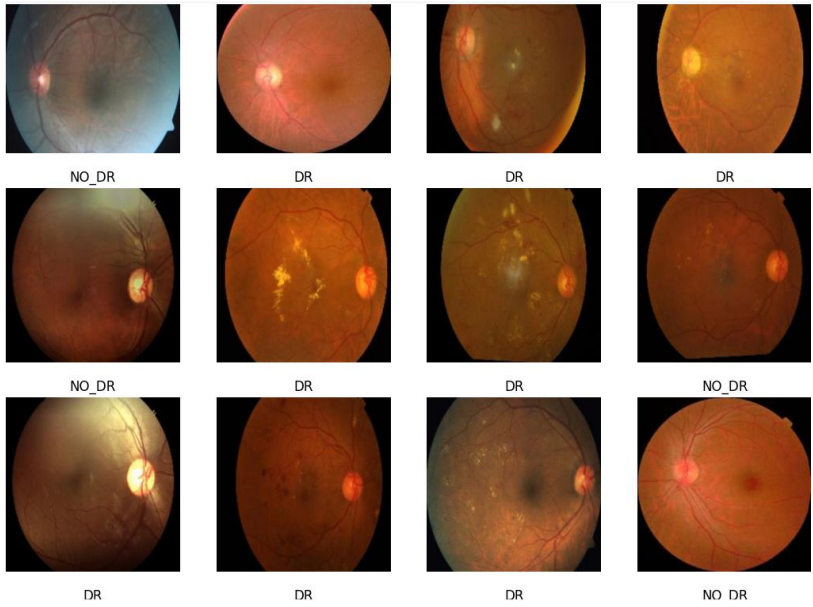


Figure 2. Sample images in Dataset1 (Darabi, 2024)

Table 1. Data distribution in classes for Dataset1

Classes	**Counts**	**Labels**
DR	1408	0
No_DR	1430	1
total	2838	

2.4.2. Dataset2: Monkeypox Skin Images Dataset

This dataset consists of images of Monkeypox, a disease rarely seen in Central and West Africa and which became an epidemic in countries outside Africa in 2022. The dataset consists of a total of 770 images divided into four different categories monkeypox, chickenpox, measles, and normal, as seen in Table 2. Sample images related to the dataset are given in Figure 3.

Figure 3. Sample images in Dataset2 (Bala et al., 2023)

Table 2. Data distribution in classes for Dataset2

Classes	**Counts**	**Labels**
Normal	293	0
Chickenpox	107	1
Measles	91	2
Monkeypox	279	3
total	770	

In the study, to eliminate the unbalanced distribution of classes in the dataset and to train the established models more healthily, the data augmentation method was applied to the dataset with an unbalanced distribution, with the number of data in each class being 300 samples. The number of samples in the dataset obtained after the data augmentation process is given in Table 3.

Table 3. Data distribution in classes for Dataset2 after data augmentation method

Classes	**Counts**	**Labels**
Normal	300	0
Chickenpox	300	1
Measles	300	2
Monkeypox	300	3
total	1200	

The ImageDataGenerator class was used for data augmentation, and the classes were balanced by applying various transformation techniques such as random rotation, shifting in width and height, cutting and shifting, zooming, and mirroring on the horizontal axis.

2.5. Deep Transfer Learning Models

Thanks to developing technologies and significant advances in the field of medicine, the variety of medical imaging techniques taken from patients for the diagnosis of diseases is increasing day by day. Images obtained from medical imaging devices such as X-ray, Magnetic Resonance Imaging (MRI), Computerized Tomography (CT), Ultrasonography, and Positron Emission Tomography (PET) and used in the diagnosis of diseases, thanks to the improvements in imaging techniques, create large data sets consisting of high-resolution complex images (Obayya et al., 2022).

Diagnosis of diseases often relies on relative evaluations and manual measurements by doctors. This situation can sometimes lead to uncertainties and errors; it can make the process of making accurate and reliable diagnoses difficult. The application of deep learning models that use multi-layered artificial neural networks to analyze large-scale complex data structures and automatically extract their features on medical images; enables the development of more effective and sensitive solutions for problems such as segmentation, disease diagnosis, and classification (Malibari et al., 2022). In this study, a study was conducted on the classification of diseases, and models were established with 6 different transfer learning methods, including VGG16, InceptionV3, ResNet50, and MobileNetV3Small and Mobile-NetV3Large from transfer deep learning algorithms.

2.5.1. VGGNet

VGGNet is an impressive CNN model introduced in the article "Very Deep Convolutional Networks for Large-Scale Image Recognition" published by Simonyan and Zisserman (2014). The model, developed by the group called "Visual

Geometry Group" at Oxford University, takes its name from the initials of its group. The model provides learning on a large dataset by undergoing a general training process and then offers a structure that can be fine-tuned for specific tasks (Bozkurt, 2021/1). In the training conducted on the ImageNet dataset, it achieved 92.7% classification accuracy with a dataset of 1000 classes containing over 14 million images, and ranked 2nd in ILSVRC 2014.

The VGGNet model, which is used as a reference in the design of later deep learning models with its modular structure and repetition of simple convolution blocks, has four different versions, VGG11, VGG13, VGG16, and VGG19, depending on the number of convolutions and fully connected layers it contains. In general, it can be said that VGG11 and VGG13 have low depth and their training times are faster; while VGG16 and VGG19 have deeper architectures and can learn more complex structures. The architecture of the VGG16 model, which consists of a total of sixteen layers, thirteen convolutions, and three fully connected layers, is presented in Figure 4.

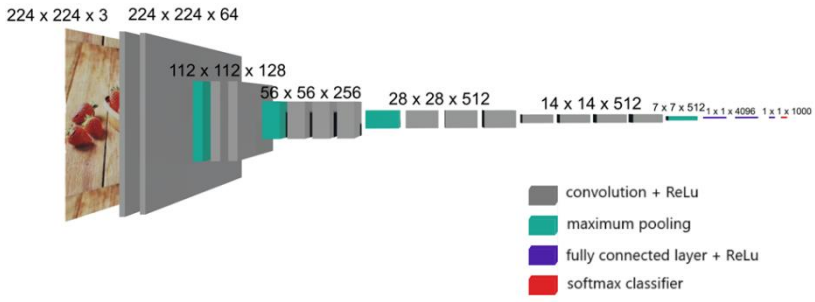


Figure 4. VGG16 architecture (Mascarenhas & Agarwal, 2021)

When we look at the architecture given in Figure 4, RGB image data of 224x224x3 dimensions are taken as the input of the model. Then, 2 convolution layers, 1 maximum pooling layer, 2 convolution layers, and 1 maximum pooling layer come in order. Then, 3 convolution layers, 1 maximum pooling layer, 3 convolution layers, and 1 maximum pooling layer are added. In the last layer, the architecture continues with a fully connected layer and ReLU activation function. In the last layer, a softmax classifier with 1000 outputs is used, as many as the number of classes in the ImageNet dataset.

The ability of the architecture to work with high-dimensional images is because the first two of the fully connected layers have 4096 neurons (Zou, Guo, & Wang, 2023). Such a large number of filters leads to costly training and problems

requiring too much data. In addition, thanks to its deep structure, the architecture generally gives successful results in large-scale image classification tasks.

2.5.2. GoogLeNet (Inception)

GoogLeNet (Inception) is a deep convolutional neural network model developed by Google researchers (Szegedy et al., 2015) to win the ILSVRC classification task. GoogLeNet, whose name refers to LeNet, the first convolutional deep learning architecture; came first in the ILSVRC 2014 competition with an error rate of 6.7%, outperforming the VGG architecture that participated in the competition in the same year.

As the depth increases in neural networks, performance also increases, but it also brings with it some difficulties such as increasing computational cost and gradient loss. Instead of simply increasing the depth, GoogLeNet uses a new concept of "starter modules" to overcome the limitations that previous CNN architectures faced in terms of depth and computational efficiency (Szegedy et al., 2015). These modules, an example architecture of which is given in Figure 5, allow the network to have multiple parallel paths with varying filter sizes, enabling features at different scales to be captured and performance to increase without an explosion in computational requirements.

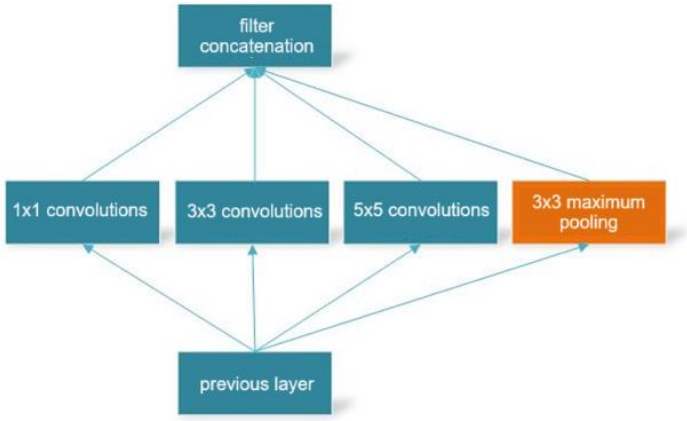


Figure 5. Inception module without dimensionality reduction (Szegedy et al., 2015)

As seen in Figure 5, in the pure version inception module introduced in the GoogLeNet (Inception) inception article, various convolution operations of 1x1, 3x3, and 5x5 sizes are applied to the input at the same time, allowing the network to capture information at different complexities and scales. Then, the outputs are combined and the results are transmitted to the next inception module. In addition, in addition to the convolution layers, the model also has a 3x3 maximum

pooling layer. Thanks to this parallel structure, in addition to high-level features, small details are also captured, and the model is provided with high performance in image recognition tasks.

In each inception module, as seen in Figure 6, 1x1 convolutional kernels are used before larger convolutional kernels and after maximum pooling, thus reducing the computational cost and the number of parameters without losing depth.

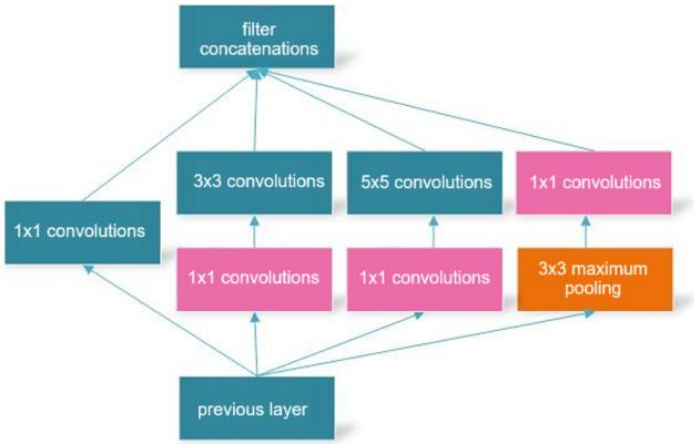


Figure 6. Inception module with dimensionality reduction (Szegedy et al., 2015)

Nine initial models with dimensionality reduction features were linearly combined to form a 27-layer GoogLeNet (Inception) model including pooling layers. The pseudo code of the model is shown in Table 3.4. In 2015 and 2016, some changes and additions were made to the basic architecture of the Inception model, and four different versions were developed: Inception v2 (Ioffe & Szegedy, 2015), Inception v3 (Szegedy et al., 2016), Inception v4 and Inception-ResNet (Szegedy, Ioffe, Vanhoucke, Alemi, & Aaai, 2017).

2.5.3. ResNet

ResNet (Residual Network) is a CNN-based deep learning architecture introduced in the article titled 'Deep Residual Learning for Image Recognition' published by He et al. (2016) The architecture aims to provide a solution to the performance degradation by adding shortcuts between layers, based on the observation that the sustainability of performance becomes more difficult as the network gets deeper (K. M. He et al., 2016). ResNet, which is 20 times deeper than AlexNet and 8 times deeper than the VGG-16 network, but has lower complexity (Xiao & Xiao, 2019), achieved a 96.43% success rate on the ImageNet dataset.

The feature that makes ResNet unique is that it contains a structure called backward transition (skip connection) or skipped connections, as shown in Figure 7. This structure is implemented by adding a skip connection passing through each layer of the network, an approach traditionally used to solve the vanishing gradient problem, one of the problems encountered during training deeper networks (Li, Wang, Liu, & Hu, 2022).

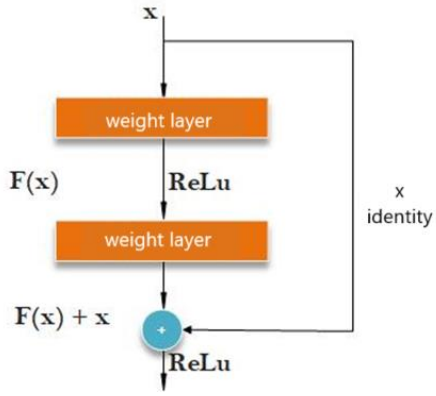


Figure 7. Residual block structure

As seen in Figure 7, the line that carries the original input x to the addition process is called a redundant connection or shortcut connection. A redundant connection is a connection that skips one or more layers. These connections create direct paths from the input to the output, so they can quickly switch between layers in the network. This feature prevents the gradient loss that occurs in the deeper layers of the network, making training more effective and speeding up the transmission of information (Meng et al., 2019).

The ResNet model has five different versions, namely ResNet18, ResNet34, ResNet50, ResNet101, and ResNet152, depending on the number of basic blocks it contains. The architecture of the ResNet50 model, which contains 50 basic blocks, is given in Figure 8.

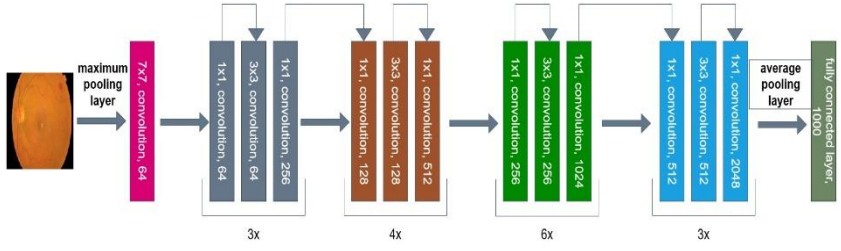


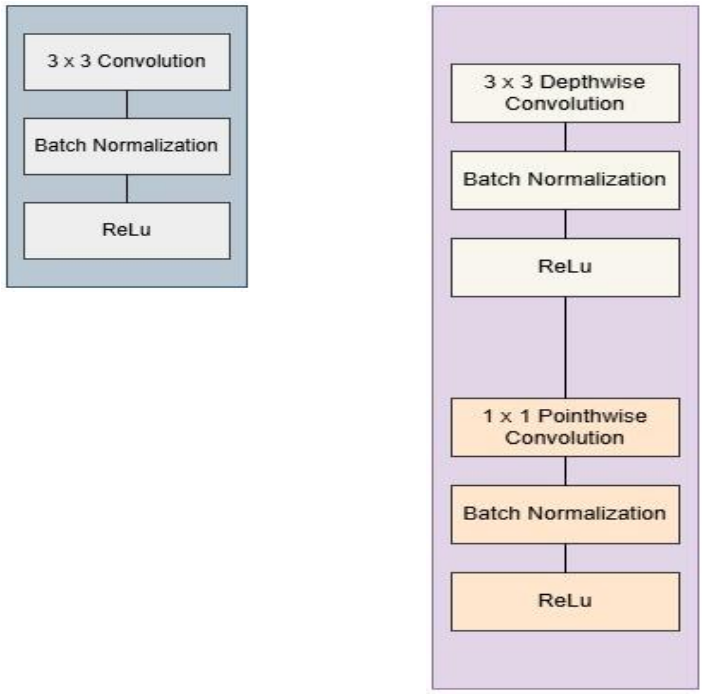
Figure 8. ResNet50 architecture (Hashmi, Katiyar, Hashmi, & Keskar, 2021)

As seen in Figure 8, the architecture consists of a total of 48 convolution layers, a max pooling layer, and an average pooling layer. The first layer is a convolution layer with 64 different kernels with a kernel size of 7x7, followed by a max pooling layer. Then, there are three convolution layers, one with 64 kernels of 1x1 size, another with 64 kernels of 3x3 size, and another with 256 kernels of 1x1 size. These three layers are repeated three times, creating a total of 9 layers. Then, there are three convolution layers, one with 128 kernels of 1x1 size, another with 128 kernels of 3x3 size, and another with 512 kernels of 1x1 size. These three layers are repeated four times, creating a total of 12 layers. Next comes three convolution layers, one with 256 kernels of size 1x1, another with 256 kernels of size 3x3, and another with 1024 kernels of size 1x1. These three layers are repeated six times, creating a total of 18 layers. Then come three convolution layers, one with 512 kernels of size 1x1, another with 512 kernels of size 3x3, and another with 2048 kernels of size 1x1. These three layers are repeated three times, creating a total of 9 layers. Finally, an average pooling operation is applied, then a fully connected layer with 1000 neurons and a softmax classifier are added, creating a network with a total of 50 layers. This architecture is designed to provide effective performance in deep learning models.

2.5.4. MobileNet

MobileNet is an efficient CNN architecture optimized for devices with limited resources. The architecture, developed by a research team at Google, was introduced in the article MobileNets: Efficient Convolutional Neural Networks for Mobile Vision Applications published in 2017 (A. G. Howard, 2017). The aim of developing MobileNet is to enable the development of deep learning-based applications on hardware with limited processing power, especially mobile devices.

Traditional deep learning architectures usually require high processing power and a large amount of energy. MobileNet was specifically designed to overcome these challenges. The size and processing load of the model are significantly reduced by using an innovative layer type called Depthwise Separable Convolution, given in Figure 9 (Hsiao & Tsai, 2021). As seen in Figure 9, this method splits the standard convolution process into two separate processes: depth-based convolution and point-wise convolution. This approach greatly reduces the computational cost while maintaining the accuracy performance of the model.



a. standard convolution layer **b.** depth separable convolutional layer

Figure 9. Depthwise separable convolution

The deep separable convolution technique used in the MobileNet architecture provides great efficiency compared to traditional convolutions. As seen in Figure 9.a, in a traditional convolution layer, each input channel is processed together with all input channels of the filters. This requires a large number of parameters in each convolution layer. In deep separable convolutions, this process is performed in two separate steps as Depthwise Convolution and Pointwise Convolution, as seen in Figure 9.b.

In the Depthwise Convolution step, a 3x3 convolution is applied to the input layer, significantly reducing the number of parameters that traditional convolutions have. In the Pointwise Convolution step, 1x1 convolution is performed, the outputs of the channels are combined, and a wider output is obtained by ensuring that the channels establish a relationship with each other. In this way, high efficiency is achieved with fewer parameters.

MobileNet is widely used in devices with hardware limitations such as smartphones, IoT devices and embedded systems thanks to its low energy consumption and efficiency. It provides low latency and resource-comparable performance to other models in tasks such as image classification, object detection and segmentation. In addition, this architecture, optimized for mobile vision applications, offers a significant advantage in time-critical tasks such as real-time image processing.

The MobileNet architecture has been improved in various aspects in the following years, making it faster, smaller and more efficient. In the MobileNetV2 version introduced in 2018, performance was improved by using inverted residual structures and linear bottlenecks (Sandler, Howard, Zhu, Zhmoginov, & Chen, 2018) The MobileNetV2 architecture has a 30% smaller size and 0.3 times faster performance compared to the MobileNet architecture.

In 2019, the MobileNetV3 model was developed by applying hardware-aware network architecture search (NAS) and NetAdapt algorithm optimizations on the MobileNetV2 architecture (A. Howard et al., 2019). The model works 2 times faster with a 30% smaller model compared to its previous version.

MobileNetV4, introduced in 2024, was designed for the ecosystem of mobile devices (Qin et al.)

Thanks to the innovations in each version, MobileNet is now considered one of the most important architectures that enable deep learning applications under limited hardware resources.

2.5.5. DenseNet

DenseNet architecture is a CNN-based deep learning architecture that aims to improve information flow and gradient propagation by establishing dense connections between layers. The architecture model, introduced in 2017 with the article titled Densely Connected Convolutional Networks, has shown its high performance on CIFAR-10, CIFAR-100 and ImageNet datasets (Huang, Liu, Van Der Maaten, & Weinberger, 2017).

DenseNet's difference from other transfer deep learning architectures is that, as seen in Figure 10, the output of each layer is directly connected to the input of all subsequent layers. In this way, more information is shared with the same number of parameters, more effective transmission of gradients is provided in backward error propagation, and thanks to the deep network it provides, it reduces the possibility of problems such as overfitting and vanishing gradient.

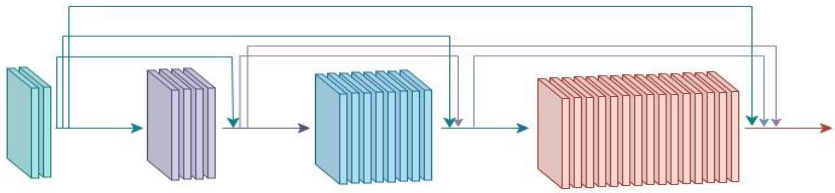


Figure 10. DenseNet

The DenseNet model has four different versions, namely DenseNet-121, DenseNet-169, DenseNet-201 and DenseNet-264, depending on the number of basic blocks (Arora, 2020). These versions increase the depth of the model, allowing better performance in more complex tasks.

3. Results and Discussion

In the study, medical image classification study was performed using six different transfer deep learning models, namely VGG16, ResNet50, MobileNetV3Small (MNv3-Small), MobileNetV3Large (MNv3-Large), InceptionV3, and DenseNet201 (DN201). The datasets used in the study were divided into 80% training and 20% test data, and in the pre-processing stage, the input dimensions were set as 224x224 for VGG16, ResNet50, MNv3-Small, MNv3-Large and DN201 and 299x299 for InceptionV3. All pixel values in the image data were scaled to the range [0, 1]. Finally, the labels were made categorical using one-hot-encoder, thus ensuring that the models could learn the classes correctly.

In the study, the genetic algorithm method was used for the optimization of the hyperparameters of the models established in the number of layers (LN), number of neurons in layers (NSL), dropout rate (DO), learning rate (LR), bach-size (BS) and epoch number (EP). The early stopping technique was applied during training to monitor the verification loss and prevent over-learning. After determining the optimum parameters, the models were tested on training and validation data sets. The optimum parameters determined by the genetic algorithm for each model are given in Table 4, and the accuracy (acc), precision (prec), recall (rec), and f1-score values obtained from the models established using the optimum parameters are given in Table 5.

Table 4. Optimum parameters determined for the models

		VGG16	ResNet50	MNv3-Small	MNv3-Large	Incep-tionV3	DN201
Dataset1	**LN**	1	1	1	2	1	2
	NSL	64	128	128	128	64	64
	DO	0.2162	0.3976	0.2207	0.2690	0.4102	0.2885
	LR	0.0005	0.0007	0.0001	0.0005	0.0004	0.0001
	BS	64	128	64	16	32	16
	EP	10	21	16	12	16	30
Dataset2	**LN**	3	3	1	1	3	3
	NSL	256	512	256	128	256	256
	DO	0.3194	0.2702	0.4527	0.4876	0.2270	0.3782
	LR	0.0001	0.0005	0.0003	0.0001	0.0005	0.0002
	BS	16	128	64	128	32	32
	EP	23	19	20	17	21	22

Table 5. Results from models

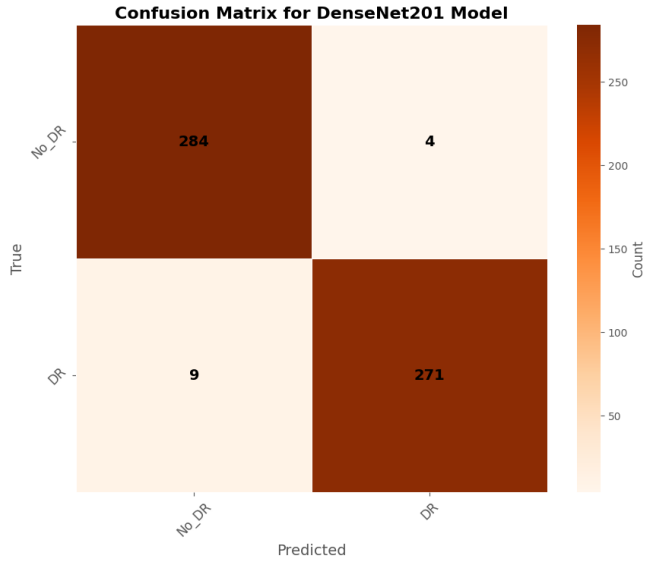
		Acc	Prec	Rec	F1-Score
Dataset1	**VGG16**	0.95	0.95	0.95	0.95
	ResNet50	0.93	0.93	0.93	0.93
	MNv3-Small	0.90	0.90	0.90	0.90
	MNv3-Large	0.88	0.89	0.88	0.88
	InceptionV3	0.97	0.97	0.97	0.97
	DN201	**0.98**	**0.98**	**0.98**	**0.98**
Dataset2	**VGG16**	0.85	0.86	0.85	0.85
	ResNet50	0.71	0.72	0.71	0.71
	MNv3-Small	0.43	0.67	0.06	0.11
	MNv3-Large	0.65	0.67	0.17	0.27
	InceptionV3	0.76	0.86	0.65	0.74
	DN201	**0.93**	**0.93**	**0.93**	**0.93**

When the hyperparameters given in Table 4 are examined, it is observed that while simple settings such as fewer layers and lower dropouts were sufficient for dataset1, more complex hyperparameter settings are needed for dataset2. VGG16 and ResNet50 architectures worked with simpler dropout rates and small batch sizes; InceptionV3 and DN201 worked with medium dropout rates and layer numbers. In the models established with MNv3-Small and MNv3-Large, deeper features were tried to be learned by selecting higher dropout rates and more layers.

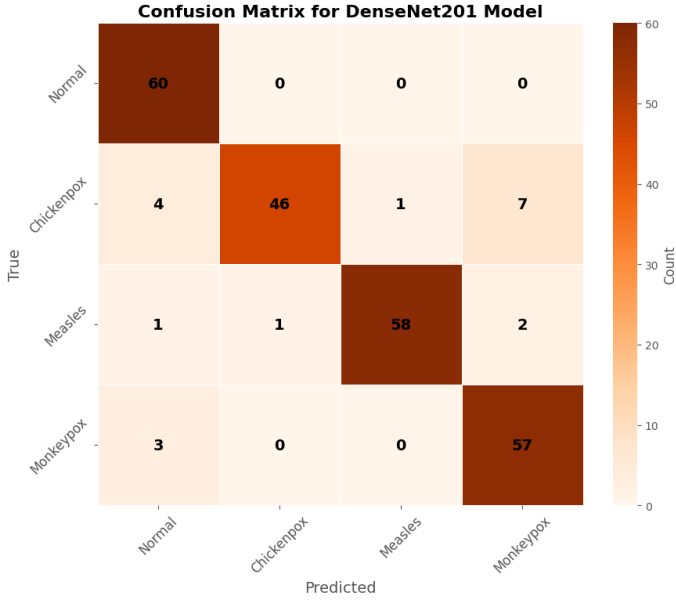
When Table 5, where the acc, prec, rec, and f1-score values of transfer learning models with hyperparameters optimized with the genetic algorithm are examined, the results obtained are listed below:

- All of the established models showed high performance in acc, prec, rec, and f1-score values for dataset1.
- When the results obtained for dataset1 are examined, the deeper DenseNet201 achieved the best results with a success rate of 0.98 in terms of four metrics.
- The model established with InceptionV3 also showed performance very close to the DenseNet201 model line with 0.97.
- MobilNet models generally showed lower performance compared to other models because they are lighter.
- Since multiple classification problems are a more complex problem, metrics in dataset2 generally have lower values compared to dataset1.
- The highest performance values for dataset2 were obtained as 0.93 when DenseNet201 was used.
- The VGG16 architecture provided balanced results thanks to its simple structure and optimized hyperparameters.
- The lowest performance values were obtained as 0.43 with the MobileNetV3Small architecture.

As a result, in the analyses performed using transfer learning models with hyperparameters optimized with the genetic algorithm, the DenseNet201 architecture showed the highest performance for both data sets, and the complexity matrices of the models created with DenseNet201 are given in Figure 11; accuracy-error graphs in Figure 12, and Roc curves and AUC scores in Figure 13.

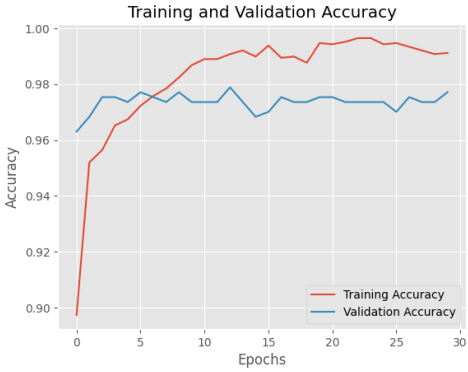


a. for Dataset1

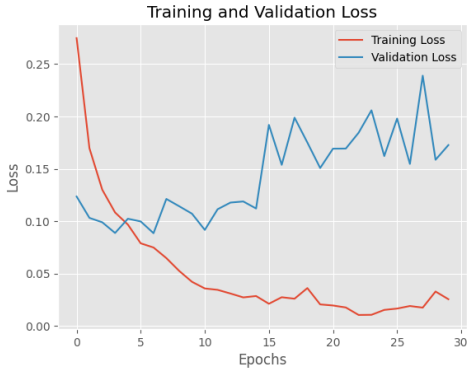


b. for Dataset2

Figure 11. Confussion matrix for DenseNet201 model

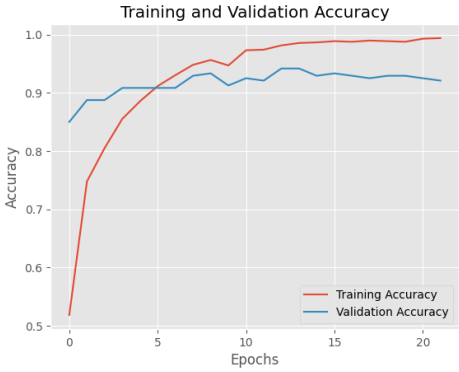


a1. accuracy for Dataset1

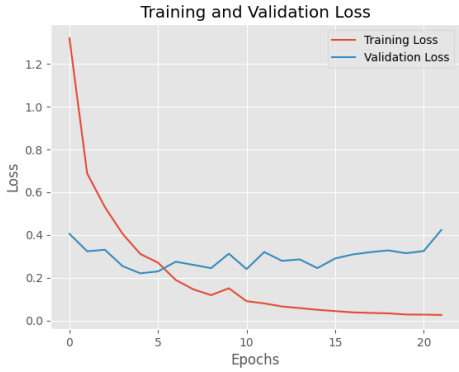


a2. loss for Dataset1

a. for Dataset1



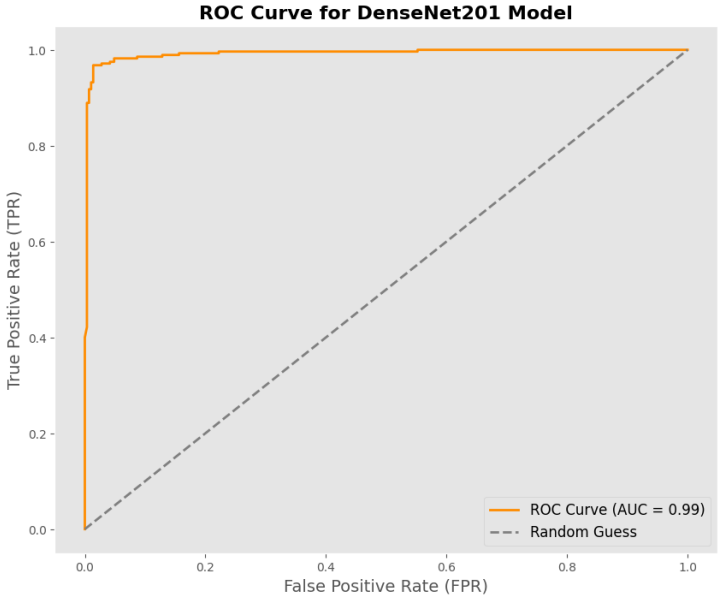
b1. accuracy for Dataset1



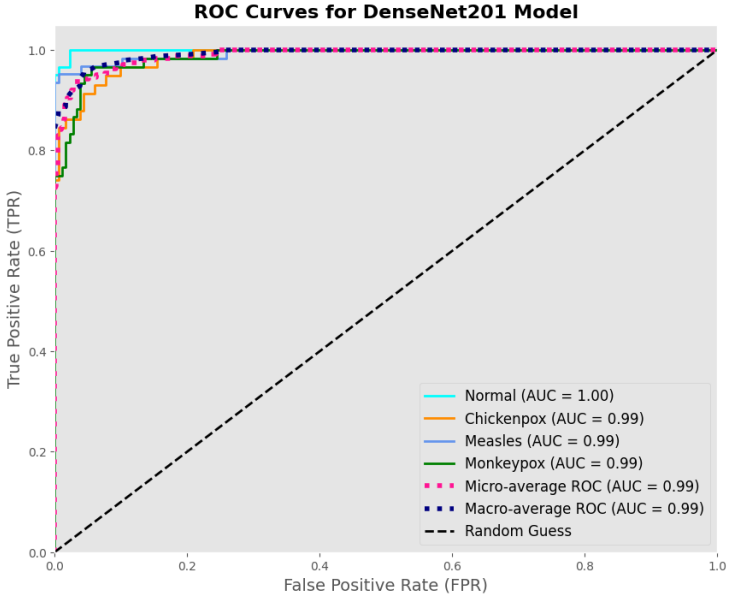
b2. loss for Dataset1

b. for Dataset2

Figure 12. Accuracy and loss grafics for DenseNet201 model



a. for Dataset1



b. for Dataset2

Figure 13. Roc curves for DenseNet201 model

4. Conclusion

Deep learning is a learning model inspired by the working principles of the human brain that enables machines to make correct decisions without any external intervention. Deep learning models show significantly higher performance in solving complex problems compared to traditional machine learning methods thanks to their training on large amounts of data.

Medical Image Processing is the process of analyzing images obtained from biomedical imaging techniques used in medicine and interpreting diseases. The increase in the quality and number of images obtained from medical imaging techniques has enabled the formation of large data sets on the subject and deep learning algorithms have begun to be used in medical image processing studies.

In this study, the hyperparameters of VGG16, ResNet50, MobileNetV3-Small, Mobi-leNetV3-Large, InceptionV3, and DenseNet201 deep learning models were optimized using genetic algorithms, and six different models were trained on two different datasets to perform medical image classification for binary classification and multiple classification problems. In the evaluations made for Dataset1, all models exhibited high performance, and the highest success was achieved with the DenseNet201 architecture. On Dataset2, which has a more complex structure, the lightweight MobileNetV3 architectures gave insufficient results, while the highest performance was again achieved with DenseNet201.

As a result, the genetic algorithm ensured that each model gave the best performance with hyperparameters suitable for the dataset, and contributed to the achievement of high success rates, especially in models established with DenseNet201.

In future studies, it is planned to test more deep learning architectures on different medical image datasets and compare the effects of different hyperparameter optimization methods other than the genetic algorithm.

References

Abdulsahib, F. I., Al-Khateeb, B., Kóczy, L. T., & Nagy, S. (2023). A transfer learning approach for the classification of liver cancer. *Journal of Intelligent Systems, 32*(1). doi:10.1515/jisys-2023-0119

Anand, V., Gupta, S., Koundal, D., Mahajan, S., Pandit, A. K., & Zaguia, A. (2022). Deep Learning Based Automated Diagnosis of Skin Diseases Using Dermoscopy. *Cmc-Computers Materials & Continua, 71*(2), 3145-3160. doi:10.32604/cmc.2022.022788

Arora, Aman. (2020). DenseNet architecture explained with PyTorch implementation from TorchVision. *Committed towards better future*.

Ayala, A., Figueroa, T. O., Fernandes, B., & Cruz, F. (2021). Diabetic Retinopathy Improved Detection Using Deep Learning. *Applied Sciences-Basel, 11*(24). doi:10.3390/app112411970

Bala, Diponkor, Hossain, Md Shamim, Hossain, Mohammad Alamgir, Abdullah, Md Ibrahim, Rahman, Md Mizanur, Manavalan, Balachandran, . . . Huang, Zhangjin. (2023). MonkeyNet: A robust deep convolutional neural network for monkeypox disease detection and classification. *Neural Networks, 161*, 757-775.

Bangyal, W. H., Rehman, N. U., Nawaz, A., Nisar, K., Ibrahim, A. A. A., Shakir, R., & Rawat, D. B. (2022). Constructing Domain Ontology for Alzheimer Disease Using Deep Learning Based Approach. *Electronics, 11*(12). doi:10.3390/electronics11121890

Chen, Yu-Ruei, Chen, Chih-Chieh, Kuo, Chang-Fu, & Lin, Ching-Heng. (2024). An efficient deep neural network for automatic classification of acute intracranial hemorrhages in brain CT scans. *Computers in Biology and Medicine, 176*, 108587. doi:https://doi.org/10.1016/j.compbiomed.2024.108587

Choi, R. Y., Coyner, A. S., Kalpathy-Cramer, J., Chiang, M. F., & Campbell, J. P. (2020). Introduction to Machine Learning, Neural Networks, and Deep Learning. *Transl Vis Sci Technol, 9*(2), 14. doi:10.1167/tvst.9.2.14

Darabi, Parisa. (2024). *Diagnosis of Diabetic Retinopathy*.

Gonzalez, Rafael C., Woods, Richard E., & Eddins, Steven L. (2020). *Digital image processing using MATLAB* (Third edition. ed.). Knoxville: Gatesmark Publishing.

Greenspan, Hayit, Van Ginneken, Bram, & Summers, Ronald M. (2016). Guest editorial deep learning in medical imaging: Overview and future promise of an exciting new technique. *IEEE transactions on medical imaging, 35*(5), 1153-1159.

Guo, Yanming. (2017). Deep learning for visual understanding. In: Neurocomput.

Hashmi, M. F., Katiyar, S., Hashmi, A. W., & Keskar, A. G. (2021). Pneumonia detection in chest X-ray images using compound scaled deep learning model. *Automatika, 62*(3-4), 397-406. doi:10.1080/00051144.2021.1973297

He, Jiajie. (2020). *Automated Detection of Intracranial Hemorrhage on Head Computed Tomography with Deep Learning*. Paper presented at the Proceedings of the 2020 10th International Conference on Biomedical Engineering and Technology, <conf-loc>, <city>Tokyo</city>, <country>Japan</country>, </conf-loc>. https://doi.org/10.1145/3397391.3397436

He, K. M., Zhang, X. Y., Ren, S. Q., & Sun, J. (2016). Deep Residual Learning for Image Recognition. *2016 Ieee Conference on Computer Vision and Pattern Recognition (Cvpr)*, 770-778. doi:10.1109/Cvpr.2016.90

Hoang, L., Lee, S. H., Lee, E. J., & Kwon, K. R. (2022). Multiclass Skin Lesion Classification Using a Novel Lightweight Deep Learning Framework for Smart Healthcare. *Applied Sciences-Basel, 12*(5). doi:10.3390/app12052677

Howard, Andrew G. (2017). Mobilenets: Efficient convolutional neural networks for mobile vision applications. *arXiv preprint arXiv:1704.04861*.

Howard, Andrew, Sandler, Mark, Chu, Grace, Chen, Liang-Chieh, Chen, Bo, Tan, Mingxing, . . . Vasudevan, Vijay. (2019). *Searching for mobilenetv3*. Paper presented at the Proceedings of the IEEE/CVF international conference on computer vision.

Hsiao, S. F., & Tsai, B. C. (2021, 15-17 Sept. 2021). *Efficient Computation of Depthwise Separable Convolution in MoblieNet Deep Neural Network Models.* Paper presented at the 2021 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW).

Huang, Gao, Liu, Zhuang, Van Der Maaten, Laurens, & Weinberger, Kilian Q. (2017). *Densely connected convolutional networks.* Paper presented at the Proceedings of the IEEE conference on computer vision and pattern recognition.

Ioffe, S., & Szegedy, C. (2015, Jul 07-09). *Batch Normalization: Accelerating Deep Network Training by Reducing Internal Covariate Shift.* Paper presented at the 32nd International Conference on Machine Learning, Lille, FRANCE.

Jahne, B. (1991). *Digital Image Processing : Concepts, Algorithms and Scientific Applications*. Berlin: Springer-Verlag Berlin and Heidelberg GmbH & Co. K Springer-Verlag distributor ,. Stephan Phillips distributor ,. DA Information Services Pty Ltd distributor ,. DA Information Services Pty Ltd distributor ,. Springer-Verlag New York Inc. distributor.

Jyotiyana, M., Kesswani, N., & Kumar, M. (2022). A deep learning approach for classification and diagnosis of Parkinson's disease. *Soft Computing, 26*(18), 9155-9165. doi:10.1007/s00500-022-07275-6

Khoei, T. T., Slimane, H. O., & Kaabouch, N. (2023). Deep learning: systematic review, models, challenges, and research directions. *Neural Computing & Applications, 35*(31), 23103-23124. doi:10.1007/s00521-023-08957-4

Laurikkala, J., Juhola, M., Kentala, E., Lavrac, N., Miksch, S., & Kavsek, B. (2000). *Informal identification of outliers in medical data.* Paper presented at the Fifth

international workshop on intelligent data analysis in medicine and pharmacology.

LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature 521*, 436-444. doi:https://doi.org/10.1038/nature14539

Li, C., Wang, Q., Liu, X. B., & Hu, B. L. (2022). An Attention-Based CoT-ResNet With Channel Shuffle Mechanism for Classification of Alzheimer's Disease Levels. *Frontiers in Aging Neuroscience, 14*. doi:10.3389/fnagi.2022.930584

Litjens, Geert, Kooi, Thijs, Bejnordi, Babak Ehteshami, Setio, Arnaud Arindra Adiyoso, Ciompi, Francesco, Ghafoorian, Mohsen, . . . Sánchez, Clara I. (2017). A survey on deep learning in medical image analysis. *Medical Image Analysis, 42*, 60-88. doi:https://doi.org/10.1016/j.media.2017.07.005

Malibari, A. A., Alshahrani, R., Al-Wesabi, F. N., Hassine, S. B., Alkhonaini, M. A., & Hilal, A. M. (2022). Artificial Intelligence Based Prostate Cancer Classification Model Using Biomedical Images. *Cmc-Computers Materials & Continua, 72*(2), 3799-3813. doi:10.32604/cmc.2022.026131

Man, K., Sabourin, V., Gandhi, C. D., Carmel, P. W., & Prestigiacomo, C. J. (2015). Pierre Curie: Contributions to Radiation Oncology and Neuroradiology. *International Journal of Radiation Oncology Biology Physics, 93*(3), E382-E382. doi:10.1016/j.ijrobp.2015.07.1521

Mascarenhas, S., & Agarwal, M. (2021). *A comparison between VGG16, VGG19 and ResNet50 architecture frameworks for Image Classification*. Paper presented at the 2021 International Conference on Disruptive Technologies for Multi-Disciplinary Research and Applications (CENTCON-2021).

McAndrew, Alasdair. (2004). *An introduction to digital image processing with MATLAB*. Boston MA: Thomson Course Technology.

Meng, Z., Li, L. L., Tang, X., Feng, Z. X., Jiao, L. C., & Liang, M. M. (2019). Multipath Residual Network for Spectral-Spatial Hyperspectral Image Classification. *Remote Sensing, 11*(16). doi:10.3390/rs11161896

Mould, R. F. (1995). The early history of X-ray diagnosis with emphasis on the contributions of physics 1895-1915. *Physics in Medicine & Biology, 40*(11), 1741. doi:10.1088/0031-9155/40/11/001

Mushtaq, Muhammad Faheem, Shahroz, Mobeen, Aseere, Ali M, Shah, Habib, Majeed, Rizwan, Shehzad, Danish, & Samad, Ali. (2021). BHCNet: neural network-based brain hemorrhage classification using head CT scan. *Ieee Access, 9*, 113901-113916.

Naz, H., Nijhawan, R., Ahuja, N. J., Al-Otaibi, S., Saba, T., Bahaj, S. A., & Rehman, A. (2023). Ensembled Deep Convolutional Generative Adversarial Network for Grading Imbalanced Diabetic Retinopathy Recognition. *Ieee Access, 11*, 120554-120568. doi:10.1109/access.2023.3327900

Obayya, M., Alamgeer, M., Alzahrani, J. S., Alabdan, R., Al-Wesabi, F. N., Mohamed, A., & Hassan, M. I. A. (2022). Artificial Intelligence Driven Biomedical Image Classification for Robust Rheumatoid Arthritis Classification. *Biomedicines, 10*(11). doi:ARTN 2714 10.3390/biomedicines10112714

Oliveira, G. C., Rosa, G. H., Pedronette, D. C. G., Papa, J. P., Kumar, H., Passos, L. A., & Kumar, D. (2024). Robust deep learning for eye fundus images: Bridging real and synthetic data for enhancing generalization. *Biomedical Signal Processing and Control, 94*. doi:10.1016/j.bspc.2024.106263

Pravin, S. C., Sabapathy, S. P. K., Selvakumar, S., Jayaraman, S., & Subramani, S. V. (2023). An Efficient DenseNet for Diabetic Retinopathy Screening. *International Journal of Engineering and Technology Innovation, 13*(2), 125-136. doi:10.46604/ijeti.2023.10045

Qin, D, Leichner, C, Delakis, M, Fornoni, M, Luo, S, Yang, F, . . . Akin, B. Mobilenetv4-universal models for the mobile ecosystem. arXiv 2024. *arXiv preprint arXiv:2404.10518*.

Qureshi, Kashif Naseer, Alhudhaif, Adi, Ali, Moazam, Qureshi, Maria Ahmed, & Jeon, Gwanggil. (2022). Self-assessment and deep learning-based coronavirus detection and medical diagnosis systems for healthcare. *Multimedia Systems, 28*(4), 1439-1448. doi:10.1007/s00530-021-00839-w

Ranjan, Amit, Lalwani, Debanshu, & Misra, Rajiv. (2022). GAN for synthesizing CT from T2-weighted MRI data towards MR-guided radiation treatment. *Magnetic Resonance Materials in Physics, Biology and Medicine, 35*(3), 449-457.

Ren, Z. Y., Zhang, Y. D., & Wang, S. H. (2022). A Hybrid Framework for Lung Cancer Classification. *Electronics, 11*(10). doi:10.3390/electronics11101614

Ruihui, M., & Xiaoqin, Z. (2019). A Review of Deep Learning Research. *KSII Transactions on Internet and Information Systems, 13*(4), 1738-1764. doi:10.3837/tiis.2019.04.001.

Samei, Ehsan, & Peck, Donald J. (2019). *Hendee's physics of medical imaging*: John Wiley & Sons.

Sandler, Mark, Howard, Andrew, Zhu, Menglong, Zhmoginov, Andrey, & Chen, Liang-Chieh. (2018). *Mobilenetv2: Inverted residuals and linear bottlenecks.* Paper presented at the Proceedings of the IEEE conference on computer vision and pattern recognition.

Sarp, S., Kuzlu, M., Wilson, E., & Guler, O. (2021). WG2AN: Synthetic wound image generation using generative adversarial network. *Journal of Engineering-Joe, 2021*(5), 286-294. doi:10.1049/tje2.12033

Siddiqui, S. Y., Haider, A., Ghazal, T. M., Khan, M. A., Naseer, I., Abbas, S., . . . Ateeq, K. (2021). IoMT Cloud-Based Intelligent Prediction of Breast Cancer Stages Empowered With Deep Learning. *Ieee Access, 9*, 146478-146491. doi:10.1109/access.2021.3123472

Simonyan, K., & Zisserman, A. (2014). Very deep convolutional networks for large-scale image recognition.

Szegedy, C., Ioffe, S., Vanhoucke, V., Alemi, A. A., & Aaai. (2017, Feb 04-09). *Inception-v4, Inception-ResNet and the Impact of Residual Connections on Learning.* Paper presented at the 31st AAAI Conference on Artificial Intelligence, San Francisco, CA.

Szegedy, C., Liu, W., Jia, Y. Q., Sermanet, P., Reed, S., Anguelov, D., . . . Rabinovich, A. (2015). Going Deeper with Convolutions. *2015 Ieee Conference on Computer Vision and Pattern Recognition (Cvpr)*, 1-9. doi:DOI 10.1109/cvpr.2015.7298594

Szegedy, C., Vanhoucke, V., Ioffe, S., Shlens, J., Wojna, Z., & Ieee. (2016, Jun 27-30). *Rethinking the Inception Architecture for Computer Vision.* Paper presented at the 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Seattle, WA.

Tabakov, M., Galus, K., Zawisza, A., Chlopowiec, A. R., Chlopowiec, A. B., & Karanowski, K. (2023). Synthetic Data Generation for Morphological Analyses of Histopathology Images with Deep Learning Models. *Vietnam Journal of Computer Science, 10*(03), 373-389. doi:10.1142/s2196888823500057

Togo, R., Ogawa, T., & Haseyama, M. (2019). Synthetic Gastritis Image Generation via Loss Function-Based Conditional PGGAN. *Ieee Access, 7*, 87448-87457. doi:10.1109/access.2019.2925863

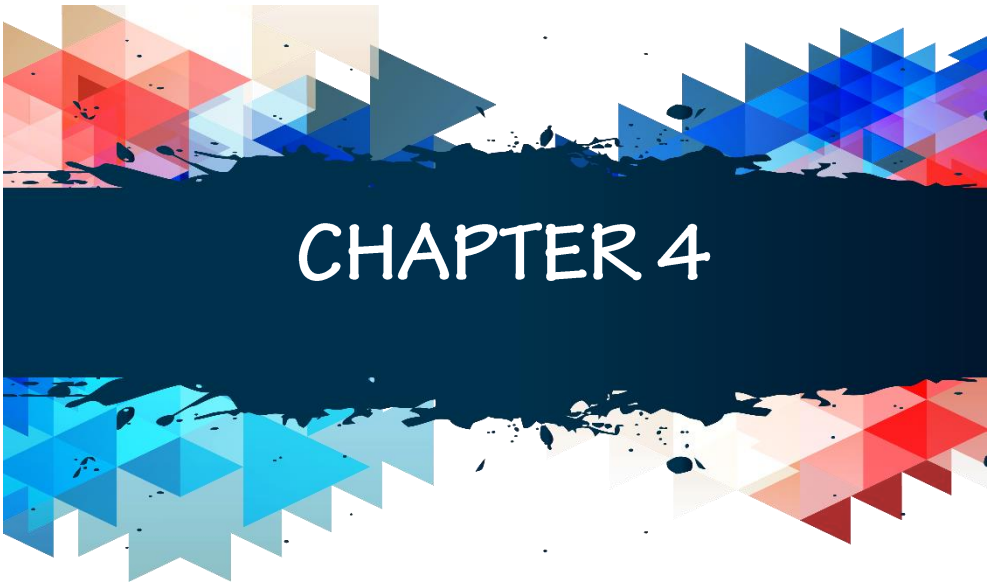
Torfi, A., Fox, E. A., & Reddy, C. K. (2022). Differentially private synthetic medical data generation using convolutional GANs. *Information Sciences, 586*, 485-500. doi:10.1016/j.ins.2021.12.018

Wang, Jiayuan, Wu, QM Jonathan, & Pourpanah, Farhad. (2023). Dc-cyclegan: bidirectional ct-to-mr synthesis from unpaired data. *Computerized Medical Imaging and Graphics, 108*, 102249.

Xiao, Y. L., & Xiao, X. (2019). An Intrusion Detection System Based on a Simplified Residual Network. *Information, 10*(11). doi:10.3390/info10110356

Yang, H., Ma, Y. H., Khan, F. G., Khan, A., & Zeng, H. (2024). HLSNC-GAN: Medical Image Synthesis Using Hinge Loss and Switchable Normalization in Cycle-GAN. *Ieee Access, 12*, 55448-55464. doi:10.1109/access.2024.3390245

Zou, J. Y., Guo, W. B., & Wang, F. (2023). A Study on Pavement Classification and Recognition Based on VGGNet-16 Transfer Learning. *Electronics, 12*(15). doi:10.3390/electronics12153370



Digital İnformation Ecosystems: A Reference Frame Model in the Layered Transformation of the Education System (LDTEIS)

***Yüksel Yurtay*[1] *& Nilüfer Yurtay*[2]**

[1] Dr., Faculty of Computer and Information Sciences, Department of Data Science and Analytics, Sakarya University, Turkey, ORCID: 0000-0003-1814-3432
[2] Prof. Dr., Faculty of Computer and Information Sciences, Department of Computer Engineering, Sakarya University, Turkey, ORCID: 0000-0002-7577-7506

1. Introduction

While technological developments continue at a dizzying pace, our routines continue to change in our social and commercial environments. The name of transforming increasing efficiency, customer experience, and operational processes into digital processes is digital transformation. Experts who have to use new technologies have to meet their needs. Commercial and industrial organizations are rapidly restructuring their systems to compete and survive. Many organizations have implemented their digital transformation plans into action [1, 2]. It excites managers in the transformation ecosystem of businesses with the confidence to compete. Mobility in the ecosystem pushes organizations to develop different products, restructure and reconsider their position in the market [3]. For organizations, digital transformation describes a series of changes such as functions, operations, goals, deep culture, workforce, technology, business models, and training [4]. Gobble [5] defines it as maximizing the effectiveness of change and opportunity by coordinating new technological approaches and tools. Starting from the definitions, everyone from employees to senior management will feel the impact of digital transformation or innovation. Innovation is a prerequisite for breathing or surviving in the digital ecosystem. Without wasting time, it is necessary to open the curtain to the light of the change experienced in every field of daily life, such as trade, production, and education. In addition to the development and adaptation of technology-based systems, the education sector should immediately be included in this process [6, 7].

Educational institutions' digital transformation is one of the most questioned systems during the pandemic process. Higher education institutions showed the first action-oriented movement of the digital transformation discourse [8–10]. If higher education institutions want to continue their existence, they need to transform together with their management and execution processes [11, 12]. So much so that educational institutions should go beyond using technological tools; managing and executing the institutional change/transformation process should be shaped according to the needs of the digital ecosystem. Transformation necessitates the change of other institutions with which it interacts. Therefore, the article presents a layered reference frame model (LDTEIS=Layered Digital Transformation Education Information System). In addition, comprehensive education system models are shared. In the context of digital transformation, the big picture of the education system is shown gradually through education processes.

The difficulties experienced in the pandemic have increased the need for higher education institutions for online education in the digital ecosystem [13, 14].

The problems encountered in online applications and institutions questioned their capabilities [15]. Experiences made the messiness and lack of coordination of solution options visible. The visibility of the problems and difficulties revealed the necessity of new technological tools and system understanding of the education system. These results suggest that educational institutions need digital transformation to exist and renew their processes [6]. Educators in the digital ecosystem will have to use sophisticated tools and methods to change their habits. What needs to be kept in mind and done is to build a new system with the awareness that the education and training process continues throughout life [6, 16].

The approach is to restructure all existing system activities related to understanding the work breakdown structure (WBS = Work Breakdown Structure) in itself. WBS manages data, access, and operations bottom-up in the transformation process [17, 18]. It is critical to make data-driven decisions and design a transparent, traceable, and accessible system to establish a frame of reference. However, careful adaptation of existing contents and processes is required. Technological infrastructure and applications used in the transformation process are critical in adaptation activities [19]. The article describes the frame of reference model (LDTEIS), which involves structuring applications and data in layers on the cloud system ground where they are securely hosted.

1.1. Teaching models in digital transformation

The SAMR model [20] provides a framework for integrating new technologies used in teaching. The transformation is structured in two levels and four stages [21]. Existing technologies are preserved, developed, modified, and redefined to align with the digital ecosystem. SAMR is adaptable and opens up new learning opportunities thanks to its technological infrastructure.

Portuguez-Castro [22] describes the distance education process, emphasizing entrepreneurial skills and abilities. Process management and execution facilitate access and control by structuring capabilities and entitlements at the social, pedagogical, technological, instructional design, and quality layers. One known reference is the technical, pedagogical content knowledge (TPCK) model [23]. It is structured on three types of information. The content is formed within the framework of technology, content knowledge, and pedagogy. With the help of technological tools, content is presented to the student at the pedagogical level. Blended learning [19] is a transformational framework but only contributes if it is aligned with the educational institution's mission, vision, and strategic goal [24]. In the teaching structure, the courses stand out in MOOC (massive open online

courses) [25] SPOC (small private online courses) formats based on LMS (Learning Management Systems). Although the focal points of the models that emerged within the scope of digital transformation studies differ, their common points are technological infrastructure and applications.

The transformation of the technological infrastructure and the system structuring at the common point can be managed and executed when adequately designed.

The transformation triggers the search for solutions for the model and makes its effects on the student visible. The model drastically changed the way individuals complete their tasks and view expectations. It is to be aware of the habits and learning actions of the student, who is defined as a digital student.

The results are evaluation of the learning process and its technological tools in sustainability.

The digital ecosystem enables students at the heart of the education system to have a richer experience while supporting learning with a deeper understanding [26]. Cloud system infrastructure comes to the fore in the practical and effective use of many new technologies, such as the Internet of Things (IoT), artificial intelligence (AI), big data (Big Data), and augmented reality (AR) in educational processes. The cloud system will be examined in detail under a separate heading, as it is the ground on which the training will take place. The use of sophisticated applications in communication, business, and social areas has proven itself in developing cloud systems infrastructure for years. Many institutions and organizations adopt cloud technologies to reduce operating costs [27–29]. Organizations working on the cloud floor increase their skills and capabilities while reducing infrastructure and management costs. The structure in which institutions and organizations' hardware, system, and application software needs are provided over the internet is known as cloud computing [30].

Digital business transformations have entered a challenging phase due to pandemic restrictions. The demand for cloud services by commerce, education, and SMEs has grown exponentially. There have been dramatic increases in video conferencing tools and primarily virtual meeting software with the challenges. It also caused a massive increase in internet bandwidth demand. Whereas in a cloud computing scenario [31], it is easy to deal with unexpected increases in bandwidth usage. In addition, in the recent past, many institutions and organizations have focused on reducing all cost items with the help of information systems (IS) and technologies (IT) [30]. The development of digital data collection, sto-

rage, analysis, reporting, and sharing capabilities under the umbrella of the enterprise is realized with information technology tools. The tools, methods, and usage patterns used differ according to the application area.

In general, framework models focus on technical issues and content such as student, teacher, pedagogy, content, educational tools, time, and usability. The model's

Location-independence and mobile access and training content are not mentioned. However, it has become critical to ensure uninterrupted service delivery with mobile devices triggered by the pandemic. LDTEIS offers a tiered approach that realizes seamless, scalable Web and mobile service.

1.2 Cloud computing and its implications

Cloud computing emerged in 2007, typically due to a standard hardware and software distribution structure [32]. By definition, it is a model that provides convenient, on-demand network access, regardless of time and space, in a shared configurable computing resource pool that can be quickly serviced with minimal management effort [27]. Cloud computing is a new computing approach in which dynamically scalable and often virtualized resources are offered as a service over the Internet [28][118]. In the era of technology evolution, cloud computing emerged as a different option in modern systems-based management where applications are run over cloud networks [29]. The first research initiatives were initiated by Google [32]. It is known that access to information and application software is provided from mobile and desktop devices, especially at every point of social life. Cloud computing provides access to software, servers, storage, data processing, and other computing resources provided by any system on the internet through a private network, in line with the company's preferences. At the same time, its configuration allows commercial and public institutions to have location-independent access to documents, e-mails, databases, and different applications. In the future, it paves the way for more efficient and effective use of the accumulated data [33]. Cloud computing provides many benefits, such as high efficiency, cost reduction, data security, scalability, access, disaster recovery, and complete control over data. Cloud system infrastructure has the potential to develop new learning models and has a widespread impact [34]. As advances in science and technology continue to reshape future business processes, the education system needs to reorganize its functions and layers. However, before adopting the cloud system, it is necessary to conduct a preliminary study by taking into account the educational structure and application differences in each country.

It defines the transformation experienced by digital technology, such as new business processes, customer experience, and changing the organizational culture for businesses trying to show their presence in global markets where competition is constantly changing. It meets the needs of institutions in communication tools/methods and business processes of the digital world, new scientific approaches, and tools. Thanks to digital world tools, corporate managers structure organizations that are flexible, dynamic, and can respond quickly to change. Businesses that survive in a structured digital ecosystem have communication skills, interact, thrive, and compete. Sector representatives demanding new technologies take different positions according to expectations and needs. However, a consensus on industry fundamentals, requirements, and uses is required.

Institutions and organizations that want to thrive and take firm steps toward the future in challenging business and competitive conditions are aware of digital transformation. In the context of the needs of information systems, cloud computing systems are in an essential position for institutions to keep up with digital transformation. Many critical needs in information systems, such as communication, accessibility, traceability, and data processing, are easily solved by cloud systems. Processing of all data defining the process in information systems and providing access to them are the most critical needs. Cloud computing systems also offer highly effective solutions for complex problems of almost every data-supported function and operation. The possibilities and experiences gained in the cloud platform are positively reflected in the business management and execution processes. As decision-makers realize the capabilities of cloud systems, they configure their organizations for digital transformation. Organizations reduce their costs and increase their efficiency by optimizing their operations and processes with the opportunities offered by cloud computing technologies.

Thanks to the robust infrastructure and low cloud computing costs, institutions and organizations gain more capabilities and flexibility. The most important source of business skills and abilities businesses is information infrastructure. Cloud computing infrastructure ensures efficient use of business resources, strategies, and processes. Thus, it provides a competitive advantage thanks to the up-to-date and effective use of cloud computing technologies.

We are witnessing the change in lifestyles, conditions, standards, and institutional order from past to present. Developments in production, health, transportation, and communication brought many innovations and conveniences to education. It has become possible for individuals who are candidates for learning at almost all ages to access information without time and place restrictions. The open availability of knowledge brings a variety of opportunities and possibilities

in education. Concepts such as access to information, open knowledge, equal opportunity, and flexibility in education are necessary [35]. It is vital for the individual to develop their knowledge and skills with their efforts, to draw a roadmap for themselves and for learning approaches. It is known to be effective in learning, especially in problem-solving and studies for a specific purpose.

The fact that strategy methods and techniques attract more attention is directly related to shaping the educational content around the programs. An inquiry-based learning approach is chosen in today's world, where access to scientific publications/content is accessible. The method defines a process based on individuals' self-learning, access to information, and cause-effect relationship. It helps develop skills such as research, definition, analysis, design, interpretation, prediction, and critical thinking in the defined process.

It is known that the understanding of education and training and the use of digital technologies also change the effects and results of learning. The positive impact of digital technologies in areas such as production and communication is seen in education. The training content and programs need to be converted in this context. This awareness will accelerate studies and transformation that will contribute to education with the wind of digital technology.

1.3. The outlook of the cloud system in digital transformation

Many businesses prepare their current initiatives with cloud platforms that adapt to future change, and convenience [32]. Cloud solutions help address current IT system limitations, digital transformation challenges, and shared cloud concerns. Choosing the right cloud meets modern cybersecurity requirements, lowers costs, and reduces the complexity of transformation [36]. By increasing the visibility of businesses, they produce the most suitable solutions for changing special needs. Companies do not want to lose their ability to intervene or take precautions against risks without disrupting the operating system while transforming. Cloud system infrastructure can meet, scale, and support functioning systematics. From this perspective, cloud systems have become a prominent component of digital transformation in commercial and industrial areas. In particular, it provides the ability for rapid and data-driven action to meet the requirements of layers and decision points in the education system.

A hybrid cloud is the name of the solution that combines the resource of public and private cloud systems. The hybrid cloud opens the door to integrated, adaptable, and cost-effective solutions. The rate of demanding businesses in business processes has exceeded 38% [37]. The hybrid cloud is mainly preferred for data privacy and hosting needs.

1.4. Contribution to cloud computing management information system

The management information system represents the communication backbone of the corporate organization. Institutions heavily use decision-making, control, coordination, analysis, and visualization processes. Therefore, almost every action within the organization finds the best solution in cloud systems' software and hardware components. Cloud systems have changed how information is accessed inside and outside the enterprise. In change transformation, managers must want to access, process, and improve real-time data.

Cloud computing technologies have four prominent advantages in management information systems.

1. It minimizes management and maintenance costs.

2. Provides access to location-independent data and information.

3. Storage saves time and effort thanks to flexibility and scalability.

4. It enables rapid compliance, coordination, data processing, and reporting.

A cloud system is an effective option for the modern management information system, which plays a vital role in the growth and development of the enterprise organization.

2. The outlook of the education system in the context of digital transformation

The meaningful aspect of the developments in digital technologies for the education system will yield much better results if appropriately adapted. The increase in their tendency toward new technologies makes it easier for them to take their future professional, hobby, and career steps [38]. Correct technological adaptation increases the competence and skills of the students in the subjects they are curious about. Ease of access to information provides the opportunity to research and experience new developments in technology. Additionally, it offers new opportunities within the education system and is a cost-effective, secure, and accessible innovation platform. Education professionals and administrators make decisions that support their insights using advanced applications and data analytics methods on cloud platforms. In Figure 1, the activities of the students receiving education services in the LDTEIS's layer have data that can be monitored and evaluated.

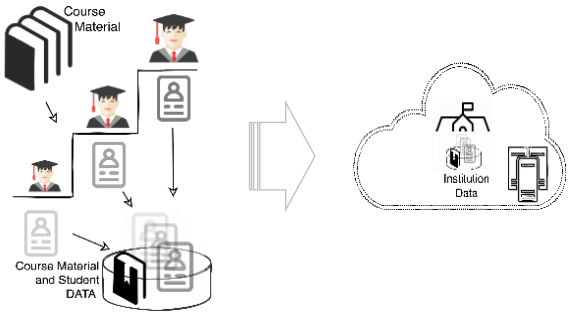


Fig 1. Consolidation of student data in LDTEIS

Consolidated data is easily refined and processed. Then, the processed information improves the course contents and the education system. With cloud computing infrastructure, new and innovative classroom environments are easily experienced. Innovative approaches such as hybrid or inverted classes are seamlessly organized through cloud technologies. Constructing education on cloud platforms will improve collaboration, traceability, capacity, flexibility, innovation, and expectations among education stakeholders [33]. As a result, actionable data of LDTEIS users' lifelong education, experience, and knowledge will be stored on cloud-based platforms.

Many experts who have given distance education exams in the recent past draw attention to the need to restructure the education system for change and transformation [35, 39]. In their study, Margianti and Mutiara say that" by providing information technology services over the cloud system, education can be more focused, the education system can be structured, and the quality of the education system can be increased [40]. Likewise, you can revolutionize your institutions if you can effectively manage all the units and activities within the education system [41]. Experiences united the experts that a gradual structural transformation should be permanent instead of temporary solutions applied to education systems. The transformation strategy is introduced gradually to capture the outputs of the value range that digital technologies can offer. Subramaniam M. [42] discussed and shared the layers of digital transformation on companies alike in his article. Figure 2 shows the education system levels in the context of traceability of LDTEIS Figure 2.

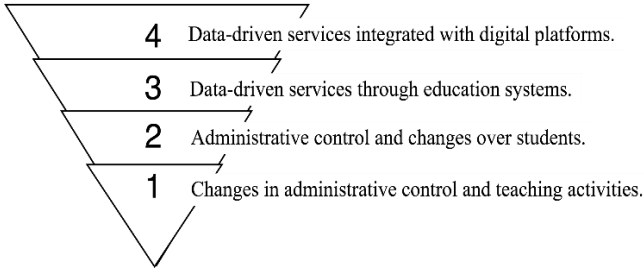


Fig 2. Education system levels

Similarly, in the context of traceability [43], the importance of transformation is emphasized in detailed studies. Because some problems, such as information asymmetry, traceability, and lack of connection in the teaching process, still await solutions [43]. In the first stage, the transformation of educational content, methodologies, education, and training stakeholders is at the center of the structuring (Figure 3).

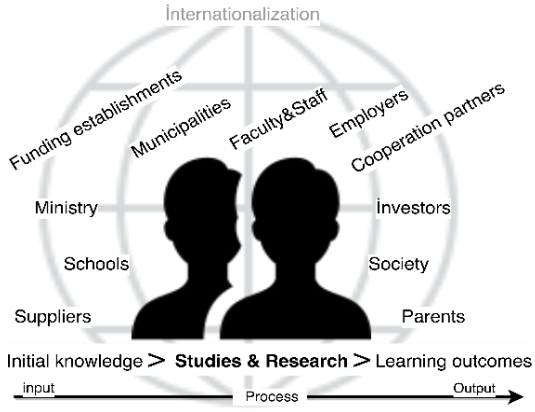


Fig 3. Education system stakeholder example [6]

Training contents, methodology, and actions of stakeholders are defined with accurate and measurable data. The stakeholders of the education system in higher education are presented in Figure 3. The role of each stakeholder is different, and their contribution to education and training activities is also different [44]. Considering the redefined roles and influences, configuring the system arises. In the first stage, educational content and teaching methodologies are reformatted and adapted to digital platforms. In the second stage, administrative activities, processes, and application software are restructured around data. In the third stage, the data is consolidated and analyzed on the system. Training services are carried out, and direction is given according to the outputs obtained through data analysis. In the fourth stage, all knowledge, skills, and acquisitions acquired outside

the educational institution are combined. The data collected around the user profile (digital profile) is stored, reported, and monitored.

2.1. Two key value factors of digital transformation

Modern digital technologies have two key-value factors at four stages of transformation [42].

- Interactive data
- Digital ecosystems

In the recent past, data has been used and collected operationally. Data is processed today, and interactive results are obtained. The consequences resulting from the interaction of the data reverse the roles of the data and the object it represents. The function that data defines and supports tends to evolve as functionality, traceability, new opportunities, and service. On the other hand, institutions and organizations need to prepare their structures for new technologies to benefit from the newly expanding role of interactive data. The possibilities provided by new technologies are necessary for the acquisition, accumulation, processing, reporting, and sharing of data. If the needs and expectations can be met in real time, the effects of possible transformation will increase even more.

For this reason, it has become necessary for institutions to move their activities to cloud computing, which is the basis of new technologies. Today, in the context of cloud computing, many institutions and organizations have begun to transform their information system infrastructure [45]. The renewed institutional and technological infrastructure will pave the way for data production and resource use. Therefore, the sensors that constitute the resources in the digital ecosystem of the near future and the data produced by the IoT-enabled connections comprise a vital work area. The consolidation and interaction of the data accumulated in the digital ecosystem facilitate the acquisition of results that support data decision-making.

LDTEIS: Layered digital transformation education information system

Implementing some solutions, especially regarding the pandemic process, is seen as the first sign of transformation. Modeling and planning a comprehensive general education system transformation ensures a seamless digital education ecosystem in the future [31]. The education system should not be left out of this transformation to meet possible future needs. As a part of the changing life, the adaptation of the education system can be realized by dividing it into stages similar to other sectors [42].

The integrated architectural structure of the education information system requires an open ground for technological developments both to provide an algorithm-based framework in data/information flow and to access more real-time information at decision points. To configure this floor with ease, LDTEIS was developed. LDTEIS provides a general framework for data/information flow infrastructure based on real-time algorithms with data consolidated from different training layers. The first layer requires that all activities that affect the student within an educational institution are measurable. Teachers have students' knowledge, skills, and assessment skills. Considering these essential processes, LDTEIS was designed from three different views.

1. Management of activity and business processes (System view)
2. Data and information flow (Information view)
3. Refined and processed data (Artificial intelligence view)

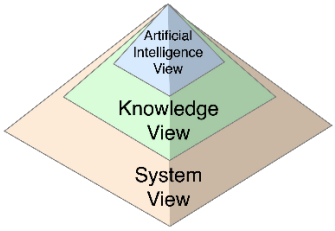


Fig 4. LDTEIS: This shows the relationship between different views

3.1. System view

The system view provides an overview of LDTEIS. The system view also shows the position of the accumulated data in each layer and the structuring related to its consolidation Figure 5. LDTEIS's architectural structure is organized as independent, flexible, open to new technologies, and manageable for educational institutions in the first, second, and third layers. In the 4th layer, the consolidation of the data accumulated at every point of individuals' business and social lives is ensured.

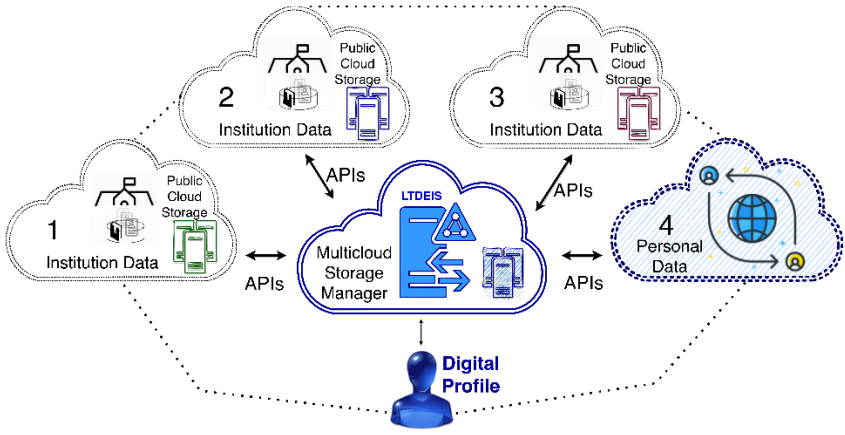


Fig 5. LDTEIS overview and digital profile

While data is collected and processed at each stage of the layers, decision-makers make data-based decisions. It consolidates the digital profile of all the information accumulated in the LDTEIS server (Multicloud Storage Manager) and processes it with artificial intelligence algorithms. The complexity and management difficulty of the education information system is overcome with the layered architecture model. Thus, access to information about the development levels of the digital profile is provided. Institutions are prepared for a digital world where educational content can be accessed, developed, and easily managed regardless of location. It provides an ideal basis for accessing the contents of institutions providing education services and the data of students/individuals. LDTEIS has encouraging features because the proposed architectural model can be quickly developed and managed, and data can be processed.

3.1.1. The four layers of digital transformation

LDTEIS is modeled from a broad perspective. Exceptional cases can / be detailed by working on the model. In the first stage, the educational content/results of the individual defined in the system and who started education in the preschool period are stored. This stage is mainly disorganized in the existing order and requires coordination. The second stage is the stage where public or private education and its results are collected in the process up to higher education. It includes the period in which documented educational data of the primary and secondary education process are collected. Integration of backlog data is a requirement. The third stage is the stage in which the higher education period, the knowledge gained in business life, and the data obtained from the previous steps are consolidated and evaluated. This stage defines the final step in which an individual's expertise matures or is determined. Data is available in the distributed

format. The final stage requires refining the data processed and accumulated across all accessible digital platforms.

In LDTEIS, the first three layers aim at institutions' dynamic and flexible development. These layers highlight activities that emphasize restructuring, identification, execution/management, reporting, and efficiency in training processes. At the same time, it aims to trigger students and instructors who take a direct role in the education process to reveal their technology-use skills and innovative thoughts. The final stage is added to each profile of action that individuals experience in the digital ecosystem they live in.

LDTEIS is defined on two introductory grounds within the digital transformation ecosystem. It is displayed in Figure 6 as an education and living ecosystem.

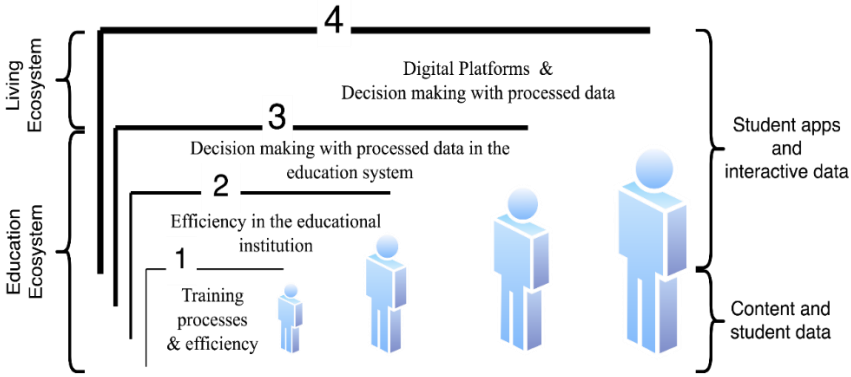


Fig 6. Four layers of digital transformation in education

In LDTEIS, data is accumulated in the education ecosystem, evaluated, and used in the living ecosystem. The education ecosystem is designed as three layers in itself. Layer One: Data from transformation on training actions and content is used and accumulated. All educational content and results received by individuals are accepted and evaluated at this stage. The first definition of the skills and abilities of the cultivated individual begins at this stage. Second Layer: It is an educational institution that actively updates the individual's profile with the institutional training and documented studies taken before higher education. It is the stage where the training data accumulated on the individual's path to expertise are processed and used. Third layer: It includes combining and using the institutions' data that make up the layer education system. The first three layers define the individual's profile in terms of development levels/results of all knowledge, skills, and achievements in the educational context. While the shape of the individual is created with data, it is also used to support efficiency, benefit creation,

and decision stages at each layer. The living ecosystem is a ground where the individual uses and increases the knowledge, skills, and abilities gained in the education ecosystem. Fourth Layer: The segment where the accumulated data is continuously and actively used/combined. In LDTEIS, skills, abilities, and experiences are defined as digital data. As in all stages, it is the point where the digital profile is updated. This layer defines an open-ended process in which the digital profile is updated using the updated and processed data. As a result, LDTEIS divides the education system into four layers against the background of student development and institutional activities. In the first, second, and third layers, the measurable values of the knowledge, skills, and abilities of the student's development are defined. The materials, tools, and contents used in the institution's educational activities are converted to be conducted remotely. The fourth layer shows the collection/processing of the student's studies outside the education layers or the data on digital platforms. The most valuable information that defines the digital profile from the data accumulated in the four layers is consolidated in the multi-cloud storage. The measurable view of the digital profile is obtained by processing the consolidated information. Table 1 shows the basic operations of the first three layers and possible digital data sources in the fourth layer. In Table 2, the measurable values of the accumulated information and the digital profile are defined.

Table 1. Main components of LDTEIS (1st,2nd,3rd Layer).

Layer	**Main Criterion**	**Sub Criterion**	
1.layer	Student development	• Mental • Physical	• Attention • Intelligence • Timing • Maturity ...
	Institution activities, contents	•Method •Learning Contents/tools •Environment	• Data collection/processing • Content/Method development • Content access • Traceability • Controllability • Class activities
2. layer	student development	• Mental • Physical	•Interest / Tendency •Skill/Ability •Awareness •Self-motivated
	Institution activities, contents	• Method • Learning Contents/tools • Environment	• Decision making with data • Tendency • Using tools and methods • Goal/Goal setting • Social and Institutional effects
3. layer	student development	• Mental • Physical	• Orientation • Using your skills • Competence • Teamwork

			• Responsibility
	Institution activities, contents	• Method • Learning Contents/tools • Environment	• Decision making with data • Social activities • Use of technological tools • Awareness
4. layer	Individual development	• Mental • Physical	• Self-planning/development • Gain experience • Proving • Specialization selection • Responsibility
		• Method • Technological tools • Scientific Methods • Environment/Interactions	• Decision making with data • Using technology and scientific method • Experiencing skills and abilities • Competence

Table 2. Main components of LDTEIS (Storage manager and digital profile).

Layer	**Main Criterion**	**Sub Criterion**	
Storage/Meta Veri	The most valuable information. Storage, consolidation, Update.	Selection and processing of updated data and extraction of meaningful information. Analysis.	Visualization / Dashboard
Digital Profile	Construction of the digital profile	Analysis and Synthesis	Visualization

The new results, both at the point of production and consumption of data, are used to guide the individuals who receive direct training gradually. The tools and opportunities used in the digital ecosystem pave the way for new structuring in the functioning of educational organizations. Therefore, reorganized institutions and employees work more efficiently and effectively. The results obtained are used effectively in orientation, decision points, and positioning in the right places of working life. In addition, disabled and non-disabled individuals who need education can access distance education services. In the context of digital transformation, the infrastructure of the education system strategy is a technology [44, 46]. With the layered structuring of educational institutions, a significant distance will be taken in the digital transformation journey. Technological transformation steps are seen as an indispensable element in educational institutions, and universities [47–49]. Decision-makers will be responsible for the physical infrastructure and training processes that carry out / manage the technical infrastructure training [31].

If the end-to-end training process is restructured correctly, expectations can be met today and tomorrow. The restructured educational approach is more resilient to risks. It is closer to emerging opportunities. Soon, decision-makers empowered by possibilities will have completed vital preparation by setting their missions correctly and redefining their visions. For this reason, the education system should define its infrastructure, stakeholders, and service content and processes that will guarantee quality education.

Cloud systems are at the heart of all organizations. In this context, it meets the expectations of the education information system. The big picture of an advanced and innovative educational information system is the structure that accepts the student in layers. For this reason, content development is critical in educational activities where mobile and remote access is at the forefront. The quality and technology of the educational content that the student access directly affects education. For example, a meaningful combination of new technological tools such as virtual reality, augmented reality, mixed reality, augmented reality, and gamification with educational processes can be used. A scalable and sustainable system is needed to promote innovation, be more agile, reduce costs, and make education processes sustainable. Thus, more effective and valuable educational content can be created. The fact that every quality educational content developed is accessible from mobile devices will have a multiplier effect on the student. As with content development, it is necessary to rework and define the roles of educators. The organization, consolidation, and sharing of data on the system are very critical in providing benefits. The system is phased in a specific order for future development, traceability, control, execution, management, and resilience to risks and anomalies.

3.2. Information view

The LDTEIS knowledge outlook indicates scientific and technological achievements. In Figure 7, LDTEIS offers its stakeholders an effective solution for data/information access between educational activities and the internet.

Institutions bring a lot of convenience in having standard educational content, improving themselves, and adapting to new technologies. It removes the obstacles in front of institutions developing content and using technology.

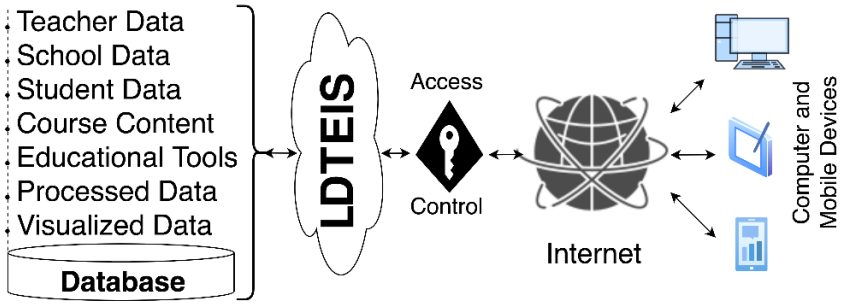


Fig 7. LDTEIS information access

LDTEIS simplifies the operations of big data organizations that are difficult to manage and trace. At the same time, it does not require a computing infrastructure. Collecting the accumulated data reduces the costs needed for its maintenance and the need for specialists. It provides an essential basis for decision-makers to obtain and support the processed data. Data, which is increasing day by day and becoming interactive, contributes more to the traceability and productivity of students. Therefore, access to data and information is as important as security and authorization. In Figure 8, two-stage switching is provided for approval and assurance.

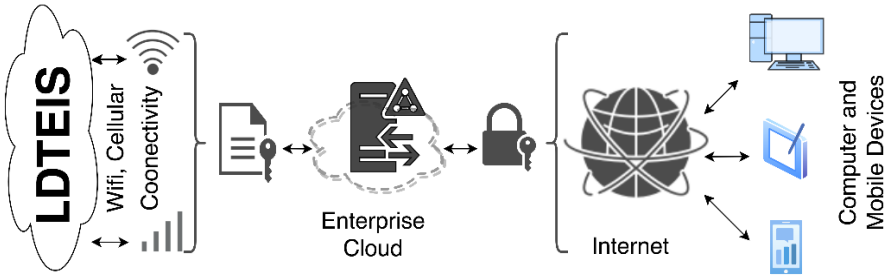


Fig 8. LDTEIS information access

This architectural design can be adapted to distributed organizations. The information-sharing mechanisms to be acquired with the LDTEIS architectural structuring are shared in Table 3.

Table 3. LDTEIS architecture information sharing mechanisms.

I.	**Information network and security**	Internet and cloud system security infrastructure
II.	**Information Forms**	Institutional Data (adaptation of inter-agency factsheets)
		Knowledge Library/Database (Enterprise archive)
		Data/Information priority relationship matrix (coding of information forms according to priority/importance)
III.	**External sources of information**	Internet-Media data/information
		Non-system educational institutions (data/information)
IV.	**Database management system**	Database management software
V.	**Visualization**	Dynamic Reports-Dashboard (Visualization of processed data)
		Standard Visualized Reports

In addition, every user/institution that provides access authorization and security has the flexibility to research and take action by providing access to data. The tools/applications required for study and processing can be easily installed on the LDTEIS model.

3.3. AI view

The artificial intelligence view was created with the idea that the accumulated data from incorporated activities and transactions will be used for automatic process improvement in the future. Thus, the AI view emphasizes the core capabilities of decision-making and the improvement of processes. It defines the refinement and processing of training data needed during the initial implementation phases of LDTEIS. Data processing/artificial intelligence applications required in this context are hosted on LDTEIS. Hosted applications are used to generate reports/information according to the requests of institutions or users. The outputs produced are visualized and used in the decision processes of the managers/users. Each requested result may differ in the training layers. Data/information communication between layers opens the door to the standardization of information forms and data processing reports. With artificial intelligence algorithms, standardized information forms and user requests will be accessed faster on LDTEIS, regardless of location.

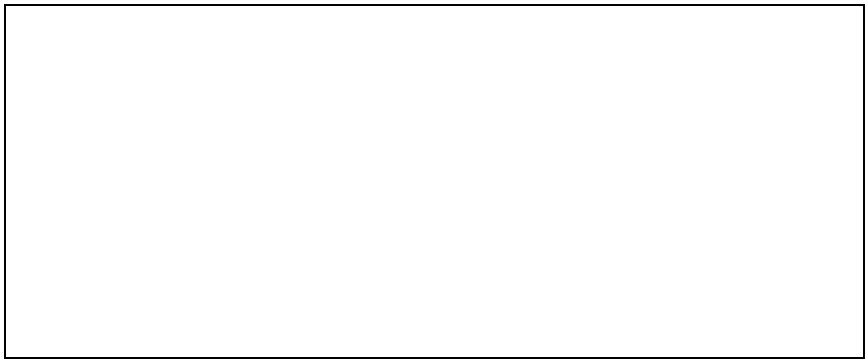


Fig 9. Decision making with data

In the future, intelligent process automation will take organizations to a different level. Instead of predefined processes, automation powered by artificial intelligence will be developed in the near future. At this point, LDTEIS prepares the operations of educational institutions for transformation.

4. Case study

This case study evaluates the Layered Digital Education Integrated System (LDTEIS) model by examining its advantages and disadvantages in the context of distance education. The analysis highlights the benefits and challenges associated with the model, particularly as it gained importance during the pandemic when the need for distance education solutions became critical. Fifteen titles listed in Figure 10 are defined as advantages and disadvantages.

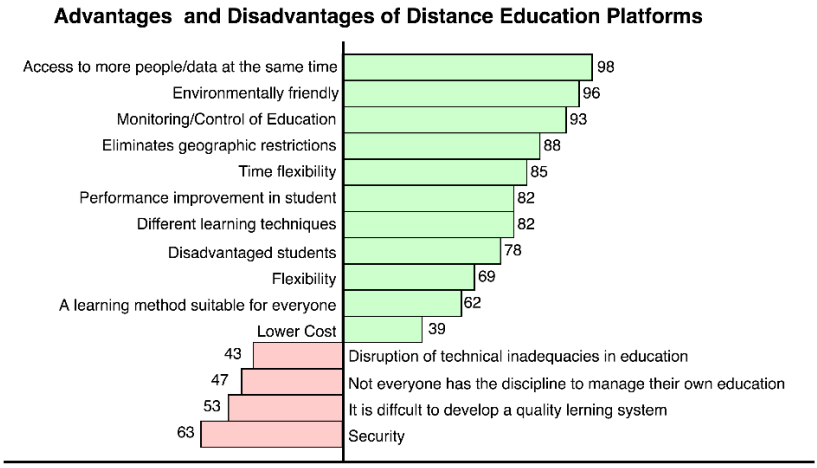


Fig 10. Case study: Advantages and disadvantages of distance education platforms

4.1. Advantages

1. Access to a Larger Audience/Data Simultaneously (98 points): LDTEIS enables many students to participate in education without geographical limitations, which is particularly beneficial in distance learning settings. This flexibility of access is one of the most significant advantages.

2. Environmentally Friendly (96 points): Distance education, facilitated by LDTEIS, reduces the carbon footprint by eliminating the need for transportation and by providing educational materials digitally, positively contributing to the environment.

3. Traceability and Control of Educational Processes (93 points): The LDTEIS model enables tracking and control of each stage of the educational process through digital tools, which allows student performance and engagement to be monitored more accurately.

4. Elimination of Geographical Restrictions (88 points): Education can take place beyond physical boundaries, allowing students to participate from any location, thus removing geographical limitations.

5. Flexibility in Time Management (85 points): Students have the flexibility to access lessons according to their schedules, providing significant advantages in time management.

6. Improvement in Student Performance (82 points): LDTEIS has shown the potential to enhance student performance in distance learning environments.

7. Support for Various Learning Techniques (82 points): Digital education platforms enable the use of a range of learning techniques and materials, allowing the model to better address students' individual learning needs.

8. Opportunities for Disadvantaged Students (78 points): LDTEIS provides educational opportunities for disadvantaged students, helping them to participate in the learning process more easily.

9. Flexibility (69 points): The model offers flexibility in managing educational processes for both students and educators, enhancing the adaptability of learning environments.

10. Suitable Learning Method for All (62 points): In general, LDTEIS is considered a flexible method that can appeal to a wide audience.

11. Cost Efficiency (39 points): Distance education offers a cost advantage; however, this benefit is rated lower compared to other advantages.

4.2. Disadvantages

1. Disruptions Due to Technical Inadequacies (63 points): Technical infrastructure issues present a significant challenge in distance education, as technological problems can disrupt students' learning processes.

2. Difficulty in Maintaining Educational Discipline (53 points): Students may find it challenging to manage their learning processes independently, which can negatively affect success in distance learning.

3. Challenges in Developing a High-Quality Educational System (47 points): Establishing quality digital education systems is demanding in terms of infrastructure and content development.

4. Security Issues (43 points): Data security and privacy concerns are critical disadvantages in distance education platforms, posing risks to student data protection.

The primary advantages of LDTEIS center around accessibility, environmental sustainability, and the traceability of educational processes. These benefits have become particularly significant in light of the increased need for distance education solutions during the pandemic. The traceability of education and the removal of geographical constraints demonstrate that distance education, facilitated by models like LDTEIS, could continue to be a sustainable option in the future.

However, LDTEIS faces challenges, primarily due to technical infrastructure deficiencies and the difficulty students may experience in maintaining self-discipline. Technical inadequacies, in particular, represent a major threat to the sustainability of distance education by causing disruptions in the educational process. Additionally, security and data privacy concerns are barriers that must be addressed for large-scale implementation.

This analysis has clearly identified the contributions and challenges of LDTEIS in distance education. The advantages of LDTEIS, including flexibility, accessibility, and environmental sustainability, make it a valuable model for digital learning environments. However, addressing technical infrastructure and security issues is crucial for further development. While LDTEIS shows great potential to enhance digital education processes in the future, its continued success depends on overcoming these challenges.

4.3. Statistical Analysis of LDTEIS Impact

In this study, a statistical analysis was conducted to meaningfully measure the effects of the Layered Digital Education Integrated System (LDTEIS) on students. The analysis focused on the system's impact on academic performance and learning progress using independent sample t-tests and ANOVA. Additionally, a satisfaction survey was used to assess students' overall satisfaction with LDTEIS.

First, an Independent Sample T-Test was conducted to compare the academic performance between the experimental group (students using LDTEIS) and the control group (students receiving traditional instruction). The results indicated a significant difference between the pre-test and post-test scores of both groups. The post-test scores of the experimental group were significantly higher than those of the control group (p ¡0.05). This suggests that LDTEIS positively influences students' academic performance, contributing meaningfully to the educational process. The use of digital learning materials and tools within LDTEIS likely facilitated better conceptual learning and improved test performance among students.

Second, a One-Way ANOVA was used to evaluate learning progress through midterm tests administered during the educational process. The results showed that students in the experimental group demonstrated significantly greater progress in the midterm tests compared to the control group (p ¡ 0.05). This finding indicates that students using LDTEIS experienced a faster and more effective learning process. The flexibility of accessing learning materials appears to have allowed students to study more efficiently and enhance their learning speed.

Finally, the Satisfaction Survey Analysis assessed the satisfaction levels of both the experimental and control groups. The Mann-Whitney U test showed a statistically significant difference in satisfaction levels, with students using LDTEIS reporting a higher satisfaction rate than those in the control group (p ¡ 0.05). The flexibility offered by the digital learning environment, personalized learning techniques, and the removal of geographical constraints contributed to increased student satisfaction. Additionally, the time management and accessibility advantages provided by the digital platform enhanced students' overall satisfaction with their educational experience.

4.4. General Evaluation

The statistical analyses conducted in this study clearly demonstrate the positive effects of the Layered Digital Education Integrated System (LDTEIS) model on student performance and satisfaction. The results from both achievement tests

and satisfaction surveys indicate that LDTEIS provides students with greater flexibility and efficiency throughout the educational process. Notably, a marked improvement in student performance was observed in the experimental group, reflecting LDTEIS's positive impact on academic success. Additionally, students using this system reported higher levels of satisfaction compared to those in traditional methods. These findings suggest that LDTEIS makes a substantial contribution to digital education processes and serves as an effective solution for enhancing efficiency in education.

LDTEIS facilitates easier access to students and data in a distance learning context. The model enables traceability and control over educational processes, regardless of location. Students can access content without time constraints, allowing for the application of various content approaches and methods. However, the main challenges include technical limitations, difficulty in maintaining student discipline, and security issues. Addressing some of these challenges, such as technical limitations, may only be possible through practical application. To mitigate security risks, LDTEIS could integrate encrypted data channels and privacy-focused protocols, which would enhance the system's scalability and reliability in broader applications.

In addition to the benefits, LDTEIS also faces certain limitations. However, the model's critical role in enabling future scientific and technological advancements in education cannot be understated. The assessment of providing distance education to even a limited sample of 18 students underscores the necessity for transformative changes in educational practices. The scope and capabilities of LDTEIS offer a promising solution to the issues seen in current distance education models, making a meaningful contribution to decision-makers and educators even if the impact cannot be fully quantified.

In conclusion, LDTEIS not only preserves the strengths of the education system but also addresses its weaknesses, allowing for proactive responses to future challenges. By integrating flexibility and control, LDTEIS offers a scalable foundation for a sustainable digital education model that can adapt to evolving educational demands.

5. Conclusion

In conclusion, integrating artificial intelligence across various education layers at decision points can effectively meet individual expectations, enhance processes, and support stakeholders at all levels. We can use current technologies to create a flexible, traceable, and agile education system with a robust communication infrastructure, enhancing system responsiveness and user interactions.

These advancements underscore the need for a reference model to support the development of an integrated, layered educational architecture. The Layered Digital Education Integrated System (LDTEIS) introduced in this study offers comprehensive architecture enabling institutions to develop their goals and content within the education layers. This model facilitates digital transformation and data structure creation within layered educational institutions, promoting coordination and cooperation across layers. The cloud-based infrastructure provides users with location-independent, real-time data access, allowing instant data sharing between institutions. Additionally, storing and processing data with artificial intelligence applications supports the progression of a smart education system. LDTEIS, thus, is a robust framework poised to meet future educational needs and complexities.

The current education models lack the responsiveness needed for instant communication, which LDTEIS addresses by providing a more agile design that keeps all processes active and responsive. Unlike traditional models, LDTEIS offers flexibility and independence to educational institutions, facilitating their development while creating a comprehensive digital profile to evaluate the education system's overall performance.

LDTEIS emphasizes data identification for all activities and stakeholders, focusing on content development through a data-driven architectural structure. This approach supports digital transformation more effectively than existing models. Furthermore, LDTEIS envisions utilizing accumulated data in its fourth layer, enabling the creation of individual digital profiles, a step beyond what current models offer.

The system ensures traceability of individual progress and achievements from the initial to the final layers, visualizing and utilizing data effectively in decision-making processes. It also opens opportunities for disadvantaged individuals to access specialized education services, enhancing their qualifications and facilitating their participation in the workforce.

LDTEIS provides an end-to-end, student-centred approach structured in four stages to meet the education system's needs both today and in the future. Its cloud-based platform offers flexibility, scalability, and accessibility, allowing for the diversification and development of educational content, including the use of augmented reality and artificial intelligence.

The system can deliver effective and practical training content for all ages and disabled groups, adapting to different expectations. It ensures that educational

activities and daily life processes are accessible and storable, bridging the gap between theory and practice.

LDTEIS supports initiatives that contribute to the digital ecosystem, particularly in the context of cloud systems and mobile technologies in education. Further research is required to meet future educational needs and adequately structure emerging standards, making LDTEIS a robust framework for the evolving education landscape.

References

[1] Brown, N., & Brown, I. (2019). From digital business strategy to digital transformation - how: A systematic literature review. *Proceedings of the South African Institute of Computer Scientists and Information Technologists 2019*, 1-8. https://doi.org/10.1145/3351108.3351122

[2] Murphy, M. P. A. (2020). COVID-19 and emergency eLearning: Consequences of the securitization of higher education for post-pandemic pedagogy. *Contemporary Security Policy*, *41*(3), 492-505. https://doi.org/10.1080/13523260.2020.1761749

[3] Hess, T., Matt, C., Benlian, A., & Wiesböck, F. (2016). Options for formulating a digital transformation strategy. *MIS Quarterly Executive*, *15/2*(131), 123-139. https://boris.unibe.ch/105447/

[4] García-Peñalvo, F. J. (2021). Avoiding the dark side of digital transformation in teaching. An institutional reference framework for elearning in higher education. *Sustainability*, *13*(4), 2023. https://doi.org/10.3390/su13042023

[5] Gobble, M. M. (2018). Digital strategy and digital transformation. *Research-Technology Management*, *61*(5), 66-71. https://doi.org/10.1080/08956308.2018.1495969

[6] App-Scoop: Digital Transformation - Next Phase for Education (2019). https://app-scoop.com/blog/digital-transformation-next-phase-for-education Accessed 2022-04-10

[7] Xu, X., Kang, J., & Yan, L. (2022). Understanding embodied immersion in technology-enabled embodied learning environments. *Journal of Computer Assisted Learning*, *38*(1), 103-119. https://doi.org/10.1111/jcal.12594

[8] Ari˜no, L.: Transformaci´on digital en la Universidad, Escola T´ecnica Superior de Enxe˜nar´ıa, CampusVida (2017). https://tic.crue.org/jornadas-crue-tic-seguridad-de-la-informacion-en-las-universidades-espanolas/Accessed 2022-04-10

[9] Serna, M. D. A., Branch, J. W., Benavides, L. M. C., & Burgos, D. (2018). Un modelo conceptual de transformación digital. Openergy y el caso de la Universidad Nacional de Colombia. *Education in the Knowledge Society (EKS)*, *19*(4), 95-107. https://doi.org/10.14201/eks201819495107

[10] Orueta, J.L., Pav´on, L.M.: Libro Blanco de la Universidad Digital 2010. Lectura Plus, Barcelona (2008). OCLC: 316144537

[11] Benavides, L. M. C., Tamayo Arias, J. A., Arango Serna, M. D., Branch Bedoya, J. W., & Burgos, D. (2020). Digital transformation in higher education institutions: A systematic literature review. *Sensors*, *20*(11), 3291. https://doi.org/10.3390/s20113291

[12] Kebritchi, M., Lipschuetz, A., & Santiague, L. (2017). Issues and challenges for teaching successful online courses in higher education: A literature review. *Journal of Educational Technology Systems*, *46*(1), 4-29. https://doi.org/10.1177/0047239516661713

[13] Daniel, S. J. (2020). Education and the COVID-19 pandemic. *PROSPECTS*, *49*(1), 91-96. https://doi.org/10.1007/s11125-020-09464-3

[14] Murphy, M. P. A. (2020). COVID-19 and emergency eLearning: Consequences of the securitization of higher education for post-pandemic pedagogy. *Contemporary Security Policy*, *41*(3), 492-505. https://doi.org/10.1080/13523260.2020.1761749

[15] Garc´ıa-Pe˜nalvo, F.J., Corell, A.: La COVID-19: .enzima de la transformaci´on digital de la docencia o reflejo de una crisis metodol´ogica y competencial en la educaci´on superior? Campus Virtuales 9(2), 83–98 (2020)

[16] Nan Cenka, B. A., Santoso, H. B., & Junus, K. (2023). Personal learning environment toward lifelong learning: An ontology-driven conceptual model. *Interactive Learning Environments*, *31*(10), 6445-6461. https://doi.org/10.1080/10494820.2022.2039947

[17] Fidalgo-Blanco, Á., Sein-Echaluce, M. L., & García-Peñalvo, F. J. (2014). Knowledge spirals in higher education teaching innovation. *International Journal of Knowledge Management (IJKM)*, *10*(4), 16-37. https://doi.org/10.4018/ijkm.2014100102

[18] Fidalgo-Blanco, Á., Sein-Echaluce, M. L., & García-Peñalvo, F. (2015). Epistemological and ontological spirals: From individual experience in educational innovation to the organisational knowledge in the university sector. *Program*, *49*(3), 266-288. https://doi.org/10.1108/PROG-06-2014-0033

[19] González, A.-B., Rodríguez, M.-J., Olmos, S., Borham, M., & García, F. (2013). Experimental evaluation of the impact of b-learning methodologies on engineering students in Spain. *Computers in Human Behavior*, *29*(2), 370-377. https://doi.org/10.1016/j.chb.2012.02.003

[20] Puentedura, R.R.: Ruben R. Puentedura's Weblog: SAMR: A Contextualized Introduction (2013). http://www.hippasus.com/rrpweblog/archives/000112.html Accessed 2022-04-10

[21] Hilton, J. T. (2016). A case study of the application of samr and tpack for reflection on technology integration into two social studies classrooms. *The Social Studies*, *107*(2), 68-73. https://doi.org/10.1080/00377996.2015.1124376

[22] Castro, M. P. (2020). *Propuesta de un modelo educativo e-learning que permita identificar habilidades de emprendimiento en estudiantes universitarios dentro de un ecosistema emprendedor.* https://doi.org/10.13140/RG.2.2.14969.39528

[23] Portuguez-Castro, M., & Gómez-Zermeño, M. G. (2020). Mentoría en curso de emprendimiento en línea.Sistematización de una experiencia en educación superior. *Formación Universitaria*, *13*(6), 267-282. https://doi.org/10.4067/S0718-50062020000600267

[24] Garc´ıa-Pe˜nalvo, F.J.: Modelo de referencia para la ense˜nanza no presencial en universidades presenciales. Campus Virtuales 9(1), 41–56 (2020)

[25] García-Peñalvo, F. J., Fidalgo-Blanco, Á., & Sein-Echaluce, M. L. (2018). An adaptive hybrid MOOC model: Disrupting the MOOC concept in higher education. *Telematics and Informatics*, *35*(4), 1018-1030. https://doi.org/10.1016/j.tele.2017.09.012

[26] SAP Insights: Education digital transformation new societal challenge(2017). https://www.digitalistmag.com/improving-lives/2017/10/05/education-digital-transformation-new-societal-challenge-05404388

[27] Mell, P., Grance, T.: The nist definition of cloud computing. National Institute of Standards and Technology (Special Publication 800-145) (2011)

[28] Furht, B., & Escalante, A. (Ed.). (2010). *Handbook of cloud computing*. Springer US. https://doi.org/10.1007/978-1-4419-6524-0

[29] Using cloud computing in higher education: A strategy to improve agility in the current financial crisis. (t.y.). *IBIMA Publishing*. Geliş tarihi 10 Aralık 2024, gönderen https://ibimapublishing.com/articles/CIBIMA/2011/875547/

[30] Hirschheim, R.A., Klein, H.-K., Lyytinen, K.: Information Systems Development and Data Modeling: Conceptual and Philosophical Foundations. Cambridge University Press, Cambridge ; New York (1995)

[31] CIOL Bureau: Growth Strategy to Accelerate Cloud Computing post-COVID-19 (2022). https://www.ciol.com/growth-strategy-accelerate-cloud-computing-post-covid-19/ Accessed 2022-04-10

[32] Krcmar, H., Friesike, S., Bohm, M., & Schildhauer, T. (2012). Innovation, society and business: Internet-based business models and their implications. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2094222

[33] Zhang, J., Zhou, J., Luo, Q., & Fan, G. (2017). *Research on the system structure of university digital campus*. 540-544. https://doi.org/10.2991/meici-17.2017.104

[34] Shevkani, K., Kaur, A., Kumar, S., & Singh, N. (2015). Cowpea protein isolates: Functional properties and application in gluten-free rice muffins. *LWT - Food Science and Technology*, *63*(2), 927-933. https://doi.org/10.1016/j.lwt.2015.04.058

[35] SALAR, H.C.: Türkiye'de ¨üniversite ¨öğrencilerinin ve öğretim elemanlarının açık ve uzaktan ögrenmeye hazır bulunuşlukları. PhD Thesis, Anadolu Üniversitesi, Eskişehir Türkiye (2013). https://acikbilim.yok.gov.tr/bitstream/handle/20.500.12812/331194 /yokAcikBilim 10004429.pdf?sequence=-1&isAllowed=y

[36] Wu, J., Shen, Q., Wang, T., Zhu, J., & Zhang, J. (2011). Recent advances in cloud security. *Journal of Computers*, *6*(10), 2156-2163. https://doi.org/10.4304/jcp.6.10.2156-2163

[37] E S Margianti & A B Mutiara. (2015). *Application of cloud computing in education*. https://doi.org/10.13140/RG.2.1.3506.0247

[38] Demir, C. G., & Yılmaz, H. (2018). Sınıf dışı eğitim faaliyetlerinin öğrencilerin bilim ve teknolojiye yönelik tutumlarına etkisi ve duygu analizi. *İnsan ve Toplum Bilimleri Araştırmaları Dergisi*, *7*(5), 101-116. https://doi.org/10.15869/itobiad.483404

[39] Thornton, T. (2014). Professional recognition: Promoting recognition through the Higher Education Academy in a UK higher education institution. *Tertiary Education and Management*, *20*(3), 225-238. https://doi.org/10.1080/13583883.2014.931453

[40] Balhareth, H. (2018). Cloud computing strategy and adoption in higher education: The case of saudi arabia. *INTERNATIONAL JOURNAL OF INFORMATION TECHNOLOGY AND MANAGEMENT INFORMATION SYSTEMS*, *9*(1). https://doi.org/10.34218/IJITMIS.9.1.2018.003

[41] 何奔奔. (2024). Research on the construction of university precision funding system from the perspective of blockchain. *Advances in Education*, *14*(02), 1421-1427. https://doi.org/10.12677/AE.2024.142220

[42] Subramaniam, M.: The 4 Tiers of Digital Transformation. Harvard Business Review (2021). Accessed 2022-04-10

[43] Riga Technical University (Riga, Latvia), Degtjarjova, I., Lapina, I., Riga Technical University (Riga, Latvia), Freidenfelds, D., & Student Union of Latvia (Riga, Latvia). (2018). Student as stakeholder: "Voice of customer" in higher education quality development. *Marketing and Management of Innovations*, *2*, 388-398. https://doi.org/10.21272/mmi.2018.2-30

[44] Quadir, B., Yang, J. C., & Chen, N.-S. (2022). The effects of interaction types on learning outcomes in a blog-based interactive learning environment. *Interactive Learning Environments*, *30*(2), 293-306. https://doi.org/10.1080/10494820.2019.1652835

[45] Faculty of Industrial Technology Bandung Institute of Technology INDONESIA, Govindaraju, R., Akbar, R., Faculty of Industrial Technology Bandung Institute of Technology INDONESIA, Suryadi, K., & Faculty of Industrial Technology Bandung Institute of Technology INDONESIA. (2018). It infrastructure transformation and its impact on it capabilities in the cloud computing context. *International Journal on Electrical Engineering and Informatics*, *10*(2), 395-405. https://doi.org/10.15676/ijeei.2018.10.2.14

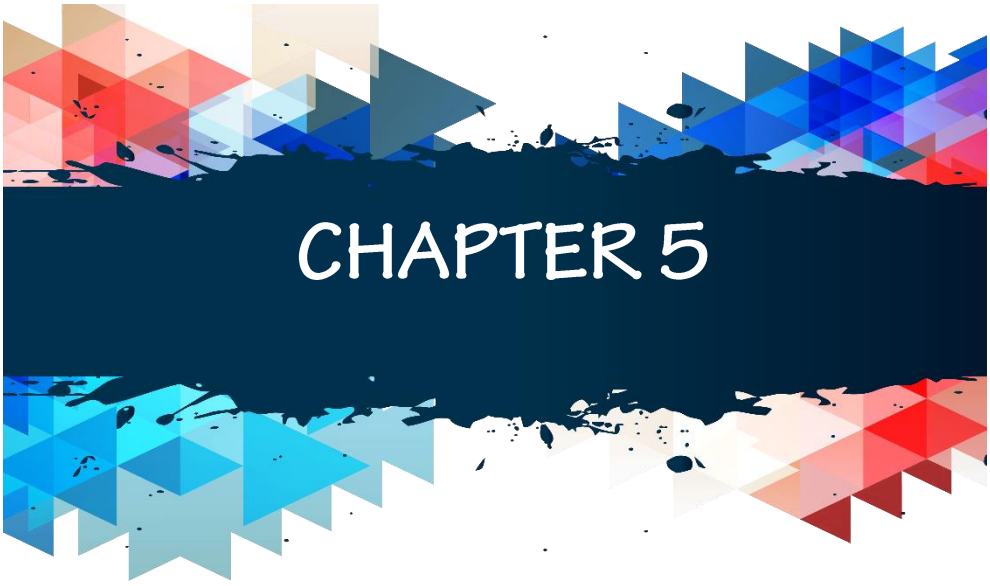
[46] Velthuis, M.P., Pav´on, L.M.: Universidad Digital (2010). In: LIBRO BLANCO DE LA UNIVERSIDAD DIGITAL 2010, Barcelona, Spain, pp. 5–27

.https://www.uladech.edu.pe/images/stories/universidad/documentos/2012/Libro-Blanco-de-la-Universidad-Digital-2010.pdf

[47] Fernández Martínez, A., & Llorens Largo, F. (2011). *Gobierno de las TI para universidades*. Madrid CRUE TIC D.L. 2011.

[48] Fern´andez S´anchez, C.M., Piattini Velthuis, M.: El gobierno y la gesti´on de las tecnolog´ıas y sistemas de la informaci´on. In: Modelo Para el Gobierno de las TIC Basado en las Normas ISO, Spain, pp. 19–28 (2012). http://www.criptored.upm.es/descarga/Extracto Modelo gobiernoTIC basadonormasISO.pdf

[49] Fern´andez Mart´ınez, A.: Impulsando el Gobierno de las TI Medianteuna Cartera de Proyectos de las TI (2020). https://prezi.com/gies0lirz3rw/cartera-de-proyectos-de-ti-en-la-universitat-dalacant/



Hash Functions: Design Paradigms, Security, and Algorithmic Analysis

***Timuçin Köroğlu*[1]**

[1] Lecturer Dr., Pamukkale University, ORCID: 0000-0002-0674-8277

1. Introduction

Hash functions convert arbitrary length data into fixed length data. If hash functions meet the criteria set for use in the field of cryptography, they are referred to as cryptographic hash functions. These functions can be used in many areas such as digital signature generation, pseudo-random number generation and authentication. (Naidu, Gorakala & Amiripalli, 2020).

Another type of hash function is non-cryptographic hash functions. These functions have a simple design due to the lack of a focus on security. This simplicity in design makes such functions operate quickly. Representing large data sizes with fixed and relatively short outputs is the key factor in making search operations highly efficient. For this reason, non-cryptographic hash functions are often used in areas where security is not required but fast access is needed. These areas include quick access to records in databases, efficient data flow in video games, dictionary structures in programming languages, and routing and balancing of data packets in computer networks (Akoto-Adhepong, Okyere-Gyamfi & Asante, 2020).

Hash functions are built upon structures that define the general framework, principles, and working methods of their algorithms. Some of the common structures include Merkle-Damgård, Wide Pipe, Tree, HAIFA, and Sponge constructions. Many traditional hash functions use the Merkle-Damgård structure. Some of these structures aim to enhance the security of Merkle-Damgård due to its vulnerabilities. However, constructions like Sponge provide a completely independent framework (Zellagui, Hadj-Said & Ali-Pacha, 2019).

A review of the literature reveals a plethora of hash functions. These functions have been subjected to rigorous analysis with regard to their security properties and vulnerabilities. Based on these evaluations, their strengths have been identified, enabling their use in various critical applications, while their usage has been abandoned in scenarios where they failed to meet requirements. The most commonly used hash functions, along with their characteristics, can be summarized as follows:

The Message Digest 5 (MD5) algorithm was designed by Professor Ronald Rivest in 1992. MD5 produces a 128-bit output. The most significant vulnerability of the MD5 algorithm is its small output size. This makes it susceptible to collision attacks, a fundamental issue where different input messages produce the same hash output. Additionally, deficiencies in the algorithm's design and hash

generation mechanism render hash codes generated by MD5 insecure. Consequently, MD5 has been deprecated by the National Institute of Standards and Technology (NIST) for password storage applications.

In 1995, the U.S. government developed the SHA-1 algorithm as part of the Capstone project. Compared to MD5, SHA-1 is slower but more resilient to brute force and other collision attacks due to its 160-bit output size. SHA-1 has been employed in several critical cryptographic protocols, including SSH, IPsec, TLS, SSL, and PGP. However, due to an increasing number of collisions in recent years, NIST prohibited the use of SHA-1 in 2013, replacing it with the SHA-2 algorithm.

The SHA-2 family is a suite of cryptographic hash functions that are a more robust alternative to its predecessors. It includes six hash functions with output lengths ranging from 224 bits to 512 bits. These functions are named based on their output length, such as SHA-224 or SHA-512. While the underlying principles of SHA-2 hash functions remain consistent across the family, certain parameters such as the number of rounds and shift amounts differ between variants. SHA-2 is highly secure for applications like digital signatures. It is frequently used in security protocols such as TLS, S/MIME, SSL, and IPsec and is also widely utilized for password hashing and cryptographic password applications.

In 2015, NIST introduced the SHA-3 algorithm as the new hash standard, following the introduction of SHA-2. SHA-3 was not designed to replace SHA-2. It was developed to address vulnerabilities arising from collision attacks in MD5 and SHA-1. Unlike MD5 and the SHA-2 family, which are based on the Merkle-Damgård construction, SHA-3 employs the sponge construction. SHA-3 is particularly well-suited for architectures where logical operations are easy and fast to implement and is frequently used in such contexts (Debnath, Chattopadhyay & Dutta, 2017).

2. Design Paradigms

2.1 Block Cipher-Based Paradigm

Block ciphers have a round function that is repeated r times and consists of simple operations. This function takes an n-bit length data as input in the first round. In each round, the function is repeated iteratively. The output obtained in the last round is the encrypted data. In each round, a key specific to that round is generated using a k-bit secret key. In round functions, decrypting the ciphertext requires the secret key to have bijective and surjective properties. There are many methods used for this purpose. The Feistel cipher is one of the most widely used

methods. According to this, the round function divides the input into two parts: left and right. The right part (R_{i-1}) forms the input for the left part (L_i) in the next round. The output obtained from the left part (Lj_{i-1}) is generated as follows: This output is obtained by adding the modified new data of R_{i-1} with the key to the left part (L_{i-1}), which is the input of the round (De Canniere, Biryukov & Preneel, 2006).

2.2 Davies-Meyer Construction

According to the Davies-Meyer design paradigm, the hash function divides the input data into equal-length segments based on the block size used by the encryption algorithm. If the length of one segment is shorter than the others, padding bits are added to make it equal in length to the other data blocks. As shown in Figure 1 , the data blocks are named $x_1,x_2,\ldots,x_j$

This paradigm consists of iterative operations performed over multiple rounds. In each round, an encryption function from the literature, such as AES or DES, is selected according to the needs of the application. In Figure 1, this function is represented by the symbol "E." For the E function, the encryption key is defined as the value of the corresponding round's x_i (i = 1, 2, ..., j).

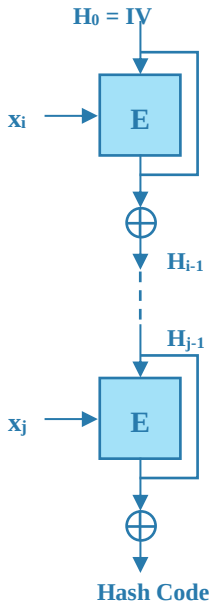


Figure 10. Davies-Meyer Paradigm Scheme

Source : (Wijitrisnanto & Susanti, 2018)

The output from the previous round is referred to as h_{i-1}. The data block x_i , which is a part of the input data to be hashed, is encrypted using the E function, producing an output h_i . This h_i value is then combined with h_{i-1} using a logical XOR operation. The resulting output becomes the input for the next round. The output obtained in the final round is the hash code. The Davies-Meyer paradigm equation is provided in Equation 1 (Wijitrisnanto & Susanti, 2018).

$$H_i = E_{x_i}(H_{i-1}) \oplus H_{i-1} \; for \; 1 \leq i \leq j, H_0 = IV \qquad \text{(Eq. 1)}$$

2.3 Merkle-Damgard Construction

The Merkle-Damgård structure aims to generate a hash function based on a compression function. The structure diagram is shown in Figure 2. Accordingly, the original data to be hashed is divided into n blocks. Each block is named from M_1 to M_n. The Merkle-Damgård structure is iterative in nature. In this structure, the output of each compression function serves as the input for the compression function of the subsequent block. However, the input to the compression function of the first block is a randomly generated data called Initial Values (IV). Each block processes the corresponding message block and the output of the previous compression function through its own compression function. In this way, all blocks are processed iteratively. The output of the final block produces the hash code of the original message (Al-Odat & Khan, 2019).

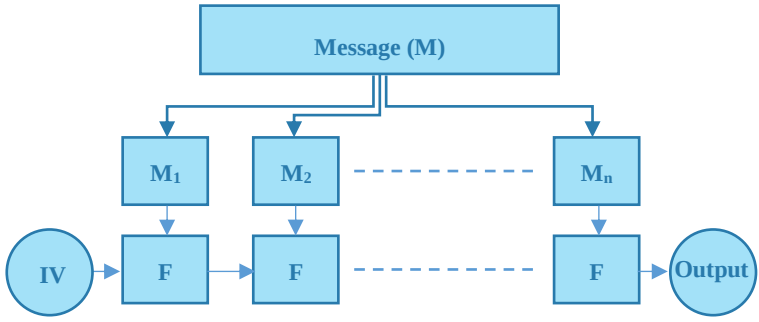


Figure 1. Merkle-Damgard Construction

Source: (Al-Odat & Khan, 2019)

2.4 The Hash Iterative Framework (HAIFA) Construction

The hash iterative framework (HAIFA) is an alternative structure that retains the core features of the Merkle-Damgård construction. The Merkle-Damgård construction has vulnerabilities against length extension attacks. HAIFA aims to eliminate this vulnerability. To achieve this, it adds extra input data to the compression function. These include an s-bit long salt value and a t-bit long counter IV value (Zellagui, Hadj-Said, 2019).

2.5 Sponge Construction

A sponge construction is capable of generating an output of arbitrary length for an input of arbitrary length. The resulting output can be employed in a variety of applications. Sponge constructions are flexibly utilised in applications such as pseudorandom number generators, message authentication codes, stream ciphers, and hash code generation. The operational process of the sponge construction is comprised of two phases: the absorbing phase and the squeezing phase.

In the absorbing phase, the M-bit message is divided into r-bit blocks. In the event that the message length is not a multiple of r, padding is applied in order to render the message length a multiple of r. The aforementioned r-bit blocks are then processed in conjunction with the S state data as input to the absorbing function. The S state consists of two parts: the r-bit portion referred to as the rate and the c-bit portion referred to as the capacity. The c-bit capacity is used to enhance security and does not directly participate in the operations. The total length of the S state is b, where b = r + c. Both the rate and the capacity parts of the S state should be initialized algorithmically, typically using predetermined or pseudo-random values.

Since the message blocks and the rate portion of the S state are both r-bits in length, their lengths are aligned. In the absorbing function, the first r-bit message block is XORed with the r-bit rate portion of the initial S state. The result of this XOR operation is combined with the c-bit capacity portion and subjected to a permutation function, producing a new S state with b = r + c. The rate portion of this updated S state is then XORed with the next r-bit message block, and the permutation function is applied again to produce another updated S state. This process is repeated until all message blocks have been processed. Upon the completion of the final message block, the absorbing phase is terminated and the squeezing phase commences.

In the squeezing phase, the user specifies the desired output length. The squeezing process is shaped according to the selected output length. The rate portion of the S state, obtained during the absorbing phase, serves as the input to the squeezing function. During this phase, the c-bit capacity is not used in any step of the squeezing function. The squeezing function applies the permutation operation to the r-bit rate portion to generate the output. If the desired output length specified by the user exceeds the r-bit length produced in the absorbing phase, the permutation process continues until the required output length is reached. Each permutation produces a separate output block, and these blocks are concatenated to form the final output of the desired length. In this way, the sponge

construction flexibly provides an output of arbitrary length as determined by the user.

The block diagram of the sponge construction is given in Figure 3 (Kumar, Gupta & Kumar, 2021).

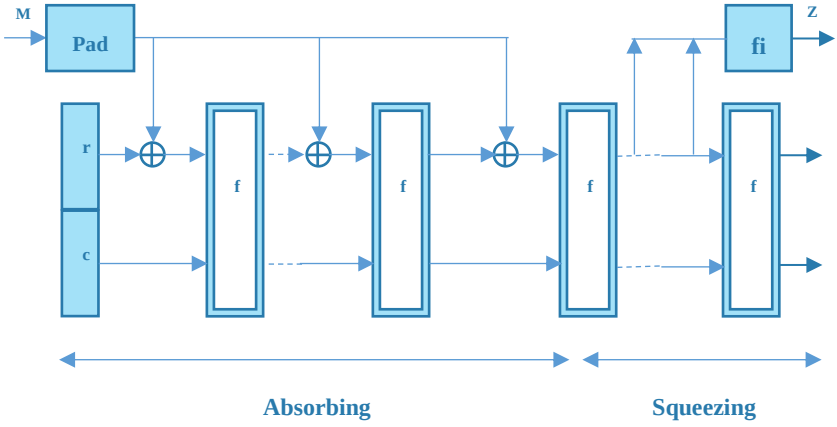


Figure 2. Sponge Construction

Source: (Kumar, Gupta & Kumar, 2021)

3. Security Features of Hash Functions

3.1 Collision Resistance

The collision resistance property in hash functions explains that two different messages should not produce the same hash output. As shown in Figure 4, if two distinct messages like *M* and *M'* have the same hash code *(H(M))*, it indicates a vulnerability in collision resistance.

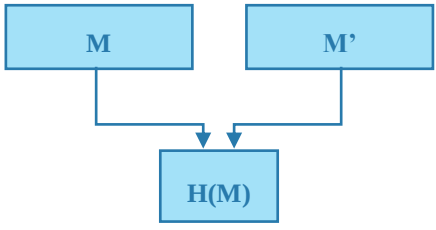


Figure 3. Collision resistance vulnerability.

Source : (Maetouq et. al., 2018)

3.2 Pre-Image Resistance

In cryptography, a pre-image is a term used to describe a message for which the hash code is known. The pre-image resistance of hash functions explains the impossibility of reaching the message (pre-image), which is unknown, by using the hash code. This situation is presented in Figure 5.

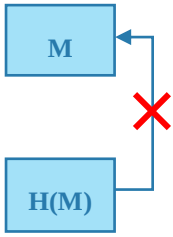


Figure 4. Pre-Image Resistance

Source : (Maetouq et. al., 2018)

3.3 Second Pre-image Resistance

Hash functions must also have second pre-image resistance. This property indicates the impossibility of finding a message different from the pre-image message (second pre-image) that produces the same hash code obtained from the pre-image message when the pre-image message and its hash code are known by the attacker. In other words, the hash code generated from the pre-image message cannot be generated by any other message different from the pre-image message. This situation is presented in Figure 6 (Maetouq et. al., 2018).

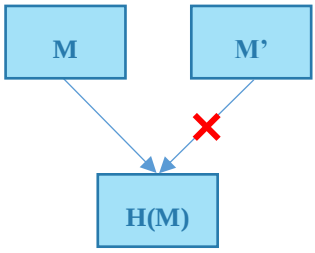


Figure 5. Second Pre-image Resistance

Source : (Maetouq et. al., 2018)

4. Review of Common and Modern Hash Algorithms.

4.1 MD5 Hash Function

The MD5 function process consists of the following steps:

The addition of padding bits is the first phase of the process. In this step, the message length is adjusted to be a multiple of 512 bits. Padding bits are used if necessary to achieve this. This can be considered separately for cases where the message length is either smaller or larger than 512 bits. If the message length is smaller than 512 bits, the message length is extended to 448 bits. The padding process starts by adding a "1" bit immediately after the end of the message, followed by adding "0" bits until the length reaches 448 bits. The remaining 64 bits store the length of the original message. Thus, the block reaches a length of 512 bits. If the message length is greater than 512 bits, the first block consists entirely of the first 512 bits of the message. The remaining length of the message always completes the blocks to 512 bits. This continues until the message length becomes less than 512 bits. When the message length is less than 512 bits, this becomes the final block, and the remaining bits of the message are padded to reach 448 bits. The remaining 64 bits contain the message length. Thus, all message blocks are always 512 bits in length, and the last 64 bits of the final block always store the message length. The padding and 64-bit message length addition steps are always performed on the last block.

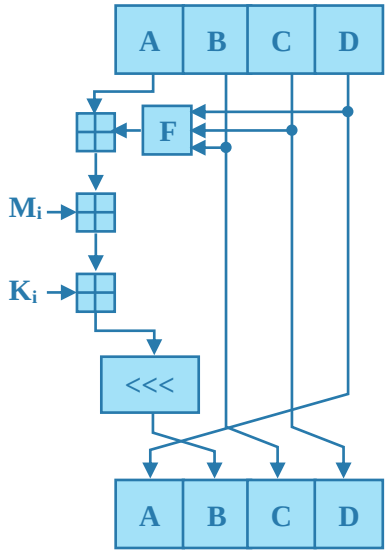


Figure 6. MD5 Hash Function Construction

Source : (Ali & Farhan, 2020)

Once the message length is adjusted to be a multiple of 512 bits, the message processing phase begins. As seen in Figure 7, the MD5 function has four buffer areas named A, B, C, and D. These buffers are each 32 bits in size, totaling 128 bits in length. This length confirms that the MD5 function produces a 128-bit output. The buffers must have initial values. These values are predetermined constants. The MD5 function uses four different functions to produce a 128-bit output. These functions are named F, G, H, and I. The buffers are updated through four rounds, each consisting of 16 steps. In each of the 16 steps, one of these four functions is iteratively applied. At the end of the four rounds, the buffers A, B, C, and D are updated for the first 512-bit block. These operations are carried out for each block. Once the final block is processed, the updated values of the A, B, C, and D buffers form the 128-bit hash code (Ali & Farhan, 2020).

4.2 Secure Hash Algorithms (SHA) Family

SHA is a family of hash functions developed by NIST. It was first proposed by NIST in 1995 under the name SHA-1. The SHA-1 algorithm, like MD5, is based on the Merkle-Damgard structure. The SHA-1 algorithm produces a 160-bit hash code. It has been used in many security applications such as S/MIME, SSL, IPSec, and PGP. However, due to flaws in its operation, it has failed to defend against collision attacks, and encryption users stopped using it after 2010. For this reason, NIST introduced the SHA-2 hash algorithm in 2002, which has versions that generate hash codes of various lengths. The SHA-2 algorithm includes a non-linear function in the compression function, making it more resilient to attacks compared to the SHA-1 algorithm (Khan et al., 2022).

4.3 SHA-2 Algorithm

The SHA-2 algorithm is based on the Merkle-Damgård structure. The construction of the SHA algorithm is shown in Figure 8.

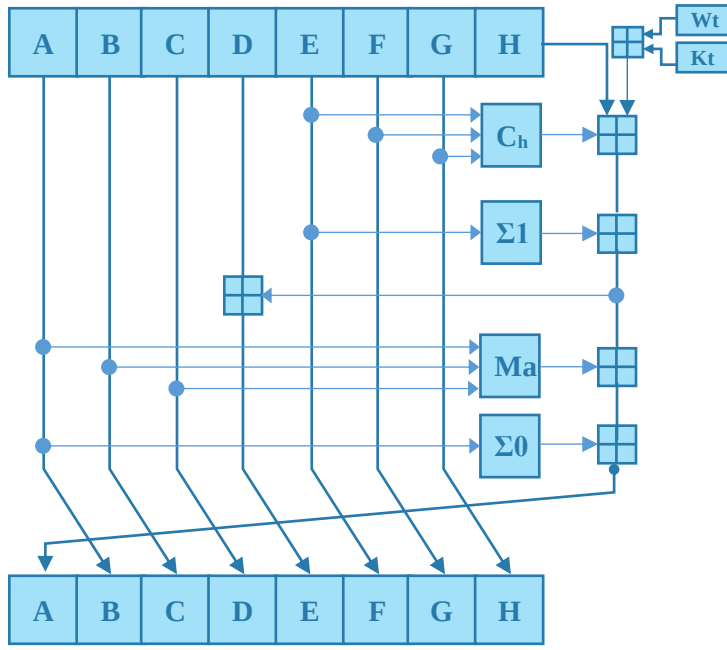


Figure 7. SHA-2 Construction
Source : (Al-Odat, Abbas & Khan, 2019)

It has different versions, such as SHA-224, SHA-256, SHA-384, and SHA-512, which produce outputs of varying lengths. SHA-2 uses eight variables: A, B, C, D, E, F, G, and H. These variables are updated iteratively with SHA compression functions and round constants over a certain number of rounds. Depending on the desired output length, the size of these variables varies. In SHA-224 and SHA-256, the variable sizes are 32 bits, and the number of rounds is 64. In SHA-384 and SHA-512, the variable sizes increase to 64 bits, and the number of rounds increases to 80.

In the SHA-2 algorithm, the process starts by dividing the message into 512-bit blocks using padding bits. In the last block, the last 64-bit section stores the length of the message in bits. After dividing the messages into blocks that are multiples of 512 bits, each block undergoes a message expansion process. Accordingly, a 512-bit message block is divided into sixteen 32-bit words. For example, in SHA-256, 48 additional 32-bit words are generated for this block. This process is called message expansion, and it is done using the function provided in Equation 2.

$$W_t = W_{t-16} + \sigma_0 + W_{t-7} + \sigma_1 \;\; 16 \leq t \leq n \quad \text{(Eq.2)}$$

The function σ0 is provided in Equation 3, and the function σ1 is provided in Equation 4.

$$\sigma_0 = RR^{r1}(W_{t-15}) \oplus RR^{r2}(W_{t-15}) \oplus SR^{r3}(W_{t-15}) \quad \text{(Eq.3)}$$

$$\sigma_1 = RR^{q1}(W_{t-2}) \oplus RR^{q2}(W_{t-2}) \oplus SR^{q3}(W_{t-2}) \quad \text{(Eq.4)}$$

In the equations, the function $RR^n(X)$ rotates the input word X to the right by n bits. The function $SR^n(X)$ shifts the input X to the right by n bits. The constants appearing in the equations for different versions of SHA are provided below.

For the SHA-224 and SHA-256 algorithms, the constant r1 takes the value of 7, r2 takes the value of 18, and r3 takes the value of 3. The other constants take values of q1 = 7, q2 = 19, and q3 = 10.

For the SHA-384 and SHA-512 algorithms, the constant r1 takes the value of 1, r2 takes the value of 8, and r3 takes the value of 7. The other constants take values of q1 = 19, q2 = 61, and q3 = 6.

$$T1 = H_{t-1} + W_t + K_t + Ch(E,F,G) + \sum_1 \quad \text{(Eq.5)}$$

$$T2 = Maj(A,B,C) + \sum_0 \quad \text{(Eq.6)}$$

$$H = G \quad \text{(Eq.7)}$$

$$G = F \quad \text{(Eq.8)}$$

$$F = E \quad \text{(Eq.9)}$$

$$E = D + T1 \quad \text{(Eq.10)}$$

$$D = C \quad \text{(Eq.11)}$$

$$C = B \quad \text{(Eq.12)}$$

$$B = A \quad \text{(Eq.13)}$$

$$A = T1 + T2 \quad \text{(Eq.14)}$$

The functions *Ch(E,F,G), $\Sigma_0(V)$, $\Sigma_1(V)$,* and *Maj(A,B,C)* are given between Equations 15 and 18.

$$Ch(E,F,G) =$$

$$(E \wedge F) \oplus (\neg E \wedge G) \quad \text{(Eq.15)} \qquad Maj(A,B,C) =$$

$$(A \wedge B) \oplus (A \wedge C) \oplus (B \wedge C) \quad \text{(Eq.16)} \sum_0(V) = RR^{r1}(V) \oplus RR^{r2}(V) \oplus$$

$$RR^{r3}(V) \quad \text{(Eq.17)} \sum_1(V) = RR^{q1}(V) \oplus RR^{q2}(V) \oplus$$

$$RR^{q3}(V) \quad \text{(Eq.18)}$$

When all rounds are completed, the variables from A to H are updated one final time, and the hash code is generated by concatenating some or all of them, depending on the SHA version. This is described between Equations 19 and 22.

$$SHA_{224} = A \parallel B \parallel C \parallel D \parallel E \parallel F \parallel G \quad \text{(Eq.19)}$$

$$SHA_{256} = A \parallel B \parallel C \parallel D \parallel E \parallel F \parallel G \parallel H \quad \text{(Eq.20)}$$

$$SHA_{384} = A \parallel B \parallel C \parallel D \parallel E \parallel F \quad \text{(Eq.21)}$$

$$SHA_{512} = A \parallel B \parallel C \parallel D \parallel E \parallel F \parallel G \parallel H \quad \text{(Eq.22)}$$

Here, it should be taken into consideration that the size of the variables is 32 bits for the SHA-224 and SHA-256 algorithms, and 64 bits for the SHA-384 and SHA-512 algorithms. Accordingly, the hash output length of the respective SHA version is calculated by multiplying the number of variables used by the length of each variable (Al-Odat, Abbas & Khan, 2019).

4.4 SHA-3 Algorithm

The SHA-3 algorithm is based on the sponge construction, which provides a secure framework for hash functions. This construction consists of two consecutive phases called absorbing and squeezing (Guitouni, Ammar & Machhout, 2024). These stages include a group of functions in which the message blocks that form the input are absorbed like a sponge and then squeezed to produce the output (Sharma & Koppad, 2016). The SHA-3 algorithm has four different versions: SHA3-224, SHA3-256, SHA3-384, and SHA3-512. In addition to these, there are extendable versions called SHAKE128 and SHAKE256. The difference of the extendable hash functions is that the output lengths can be adjusted (Kuila, Chawdhury & Pal, 2015).

The differences between the versions of the SHA-3 algorithm are given in Table 1 based on output lengths, r=bit rate, and c=capacity (Dolmeta, Martina & Masera, 2023).

Table 5. SHA-3 Algorithms

Algorithm	Output (Bits)	Rate r (Bits)	Capacity c (Bits)
SHA3-224	224	1152	448
SHA3-256	256	1088	512
SHA3-384	384	832	768
SHA3-512	512	576	1024

Source : (Dolmeta, Martina & Masera, 2023)

4.5 BLAKE Algorithm

BLAKE is a hash function based on the ChaCha stream cipher algorithm, modified and adapted from this algorithm. It has four different versions depending on the word size used in its internal mechanism and the lengths of the hash codes they produce. Among these, BLAKE-224 and BLAKE-256 use 32-bit words. BLAKE-224 produces a 224-bit hash code, while BLAKE-256 produces a 256-bit hash code. BLAKE-384 and BLAKE-512 use 64-bit words. BLAKE-384 produces a 384-bit hash code, while BLAKE-512 produces a 512-bit hash code.

The BLAKE algorithm was submitted by its designers to the hash function competition organized by NIST. In 2012, BLAKE was one of the last five finalists. However, the algorithm named KECCAK won the competition. Later, a new version based on the BLAKE algorithm, called BLAKE2, was introduced on December 21, 2012, as a strong alternative to the MD5 and SHA-1 algorithms. BLAKE2b demonstrated high performance compared to many hash function algorithms on 64-bit x86 and ARM-based architectures.

BLAKE2 is also more secure than the SHA-2 algorithm. BLAKE provides very strong resistance to length extension attacks and shares similar characteristics with SHA-3 in terms of indistinguishability from a random oracle. Some variants of BLAKE2 show better performance on multi-core systems (Sadeghi-Nasab, Rafe, 2023).

Blake-3 algorithm is an improved version of the previous BLAKE versions. BLAKE3 provides better security and performance compared to its predecessors. It also supports SIMD architecture. BLAKE-3 produces a 512-bit hash code. BLAKE-3 divides the message to be hashed into fixed-size chunks and summarizes these chunks within a tree structure. This working principle is suitable for

parallel processing and provides significant performance improvement on large data blocks (Tajane et al., 2024).

4.6 Argon2 Algoritm

Passwords, despite their drawbacks such as low entropy, continue to maintain their dominance in authentication applications in many web services. To enhance password security, designers have developed many methods. Among these, hash code generation processes, which gained speed as a result of Moore's Law, have been deliberately invoked multiple times. Thus, attackers' password cracking has been made more difficult due to increased time costs and similar reasons.

In response, password crackers have started to use new architectures such as high-performance GPUs, FPGAs, and ASICs. It has been determined that these architectures are effective in applications requiring low memory but struggle in applications requiring high levels of memory usage. This situation has provided an advantage for designers developing defense mechanisms against attackers and made attackers' work more difficult with architectures requiring high amounts of memory.

The Argon2 hash algorithm aims to maximize memory write performance and the efficiency of parallel usage of processing units. This goal is related to performance and is used in applications where performance is required. However, in addition, the Argon2 algorithm can offer different approaches with its methodology that uses memory more intensively than necessary to prevent the relationship between the processor and memory from being deciphered by attackers, especially in applications vulnerable to tradeoff attacks. This makes it more secure. Since Argon2 is designed to work on the x86 architecture, it uses modern AMD and Intel processors. This enables the utilisation of the cache and memory organisation structure of these processors.

Argon2 has two different versions: Argon2d and Argon2i. Argon2d focuses on performance and is faster. Side-channel timing attacks can be effective on algorithms with data-dependent memory access. Therefore, Argon2d is more suitable for such applications that are not affected by these attacks, such as cryptocurrencies. Argon2i, unlike Argon2d, does not use data-dependent memory access. Instead, it uses data-independent memory access. This allows the Argon2i algorithm to organize memory in a way that increases security. Thus, it prevents the relationship between the data exchange between the processor and memory from being deciphered by attackers. For this reason, Argon2i provides better protection against tradeoff attacks. Considering all these, Argon2i is slower than the Argon2d algorithm but more secure (Biryukov, Dinu & Khovratovich, 2016).

5. Artificial Intelligence and Hash Functions

The development of the internet and the information age has led to the extraordinary growth of multimedia data such as images, videos, and audio on the internet. This growth has brought along the problem of searching and retrieving this data in an intelligent and fast manner. The search for multimedia data on the internet requires multimodal retrieval. This is, in a sense, a data similarity search and a Nearest Neighbor (NN) search problem. That is, when a query is performed on a dataset, the multimedia data most similar to each other is returned. However, another problem here is that multimedia data requires large storage space and time-consuming queries. Therefore, storing this high-dimensional data as hash codes, which are a concise summary of the data, and ensuring the best representation in terms of similarity between these codes and the high-dimensional data could be a solution. For this solution, deep hashing research has significantly increased in recent years, yielding successful results (Cao etc al., 2020).

Artificial intelligence-driven hashing algorithms can be divided into two categories: data-independent and data-dependent methods.

Data-independent methods are implemented without analyzing or involving the content of the data in the process. These methods are divided into two categories: projection-based methods and deterministic structure-based methods. Since these are grouping methods independent of the data, they do not classify hash codes according to the content of the data.

Data-dependent methods, where the distribution and label information of the data are used in the design of the hash function, are referred to as hash learning. In this method, since the content and features of the data are included in the process, hash codes are generated in a way that classifies the original data. In a sense, for data such as images that could belong to the same category, hash codes that are close to each other are generated. Hash learning is divided into two subcategories: supervised and unsupervised.

In the supervised method, hash learning is performed using the labeling of similarities between data and the label information. In the unsupervised method, hash learning is carried out based on the structure of the data without using label information.

Traditional artificial intelligence methods are not at the desired level in generating hash codes based on image features in large datasets and classifying them according to these features. Deep learning-based hash methods can overcome this problem.

Deep learning methods can detect multiple features of images to be classified and present the parametric values of these features in a way that improves the success of hash learning. Thus, images are represented with appropriate hash codes corresponding to their labels.

Deep hashing uses deep neural networks in hash learning. Among deep neural networks, deep convolutional neural networks (CNN), which are frequently used in image processing applications, are one of them.

Deep hashing methods consist of four components:

- A fully connected convolutional artificial neural network. The goal is to extract image features,
- A hashing layer necessary to best represent the image with hash codes,
- A loss function that can generate similar hash codes for similar images,
- A quantization loss that performs hashing quality control.

In deep hashing methods, the similarity of the produced hash codes is calculated using the Hamming distance (Singh & Gupta, 2022).

6. Qantum Hashing

Quantum computers promise to solve complex problems in a much shorter time and with less energy consumption. However, this positive aspect may lead to some negative consequences for society. The reason is that these positive features of quantum computers can serve as a hidden resource for attackers to decrypt cryptographic security (Hatanaka etc al., 2024).

The term "computationally difficult problem" refers to the notion that there must not exist any algorithm capable of reaching a realistic solution for the problem, other than an algorithm that enumerates all possible instances compatible with the solution. Traditional cryptographic functions aim to produce secure and attack-resistant solutions by leveraging the hardness of mathematical problems such as discrete logarithms and integer factorization. The main challenge here is to prove that a problem, deemed computationally difficult, is genuinely hard.

While traditional cryptographic functions are based on these approaches, quantum cryptography seeks to develop solutions that are grounded in the principles of quantum mechanics. In recent years, a considerable number of quantum one-way function models have been put forth for consideration. Quantum one-way functions can be classified into two principal categories.

The first category includes functions where both the input and the output are binary data, referred to as classical-classical functions. Although these functions

use classical inputs and produce classical outputs, they are designed to remain difficult to invert even for quantum systems.

The second category consists of functions called classical-quantum one-way functions. The main difference between classical-classical and classical-quantum functions is that, in the latter, the input is classical binary data, while the output is a quantum state (Ablayev & Vasiliev, 2013).

7. The Common Usage Areas Of Hash Functions

7.1 Message Authentication

Hash functions play a vital role in ensuring secure communication in modern cryptography in many areas. These include authentication in data access, monitoring data integrity, password protection, forensic investigations, pseudorandom number generation, and blockchain. One of the important areas where hash functions are used is message authentication. Message authentication checks whether a message transmitted over the network has been altered during the transmission process. Message authentication can be achieved using a Hashed Message Authentication Code (HMAC) generated from the original message. The generated hash code is transmitted independently along with the original message over the network. The recipient reproduces the hash code of the received message using the same cryptographic hash function and secret key. The generated hash code is compared with the received hash code. If the hash codes match, it is understood that the integrity of the message has been preserved.

HMAC consists of a hash code generated with one of the hash functions and a cryptographic key. The cryptographic key is used during the generation process of the hash code from the original message. Thus, only the recipient with the cryptographic key can check the integrity of the received data. The quality of HMAC is directly proportional to the quality of the hash function used, the length of the hash code, and the size/quality of the key (Upadhyay etc al., 2022).

7.2 Digital Signature

Nowadays, digital signatures are being used more frequently in parallel with the development of technology and are replacing wet signatures (Genç & Afacan, 2021).

In digital signature systems, signature calculation processes are performed on the fixed and small-sized hash code of the original message. If the verification of the hash code of the signed message received by the recipient is successful, the message integrity and signature are considered valid.

7.3 Password Verification

Access to resources is provided through user-defined passwords. Storing passwords in plaintext creates a security vulnerability that can lead to extremely severe consequences. This significant security vulnerability can be mitigated by converting passwords into hash codes and storing them in this form. In this case, user authentication in password-protected access is carried out as follows: The user's password securely reaches the recipient. The password is rehashed on the recipient's side. This hash is compared with the hash stored on the recipient's side. If the hash outputs match, the user is authenticated.

Cryptographic hash functions can produce hash codes at high speeds due to advanced graphics processing units and speed-focused architectures. However, this situation allows attackers to make a high number of password guesses in very short periods to crack passwords. To prevent this, random data called "salt" is processed with hash codes to randomize the resulting hash outputs. In this way, it becomes much more difficult for attackers to guess passwords (Sadeghi-Nasab & Rafe, 2023).

7.4 Blockchains

Blockchain, one of today's popular technologies, uses hash functions to ensure the integrity of the distributed ledger within its structure. The blocks within the blockchain structure are represented by hash codes. Each block adds its hash digest to the subsequent block. In this way, blocks are logically linked to each other. In this structure, if the internal values of one of the blocks are modified, the hash values of all subsequent blocks connected to it become invalid. SHA-256, a variant of the SHA-2 hash algorithm, is preferred in many blockchain technologies due to its security and computational efficiency. The integrity of the ledger in blockchain technology depends on the collision resistance of the hash function it uses (Martino & Cilardo, 2019).

7.5 Internet of Things (IoT)

Internet of Things (IoT) devices are not suitable for use with algorithms that require high resource demands, such as Advanced Encryption Standard (AES) or Rivest-Shamir-Adleman (RSA), due to their limited resource management, such as low-capacity processors and small data rates. If used, issues such as inefficient performance and rapid battery consumption may arise. In studies conducted in the 2000s, it was predicted that the hybrid use of traditional hash functions with lightweight block ciphers could be a solution (Gunathilake, Al-Dubai & Buchana, 2020).

8. Comparison of Hash Functions

In Table 2, information about the message block lengths, the number of rounds, the word size used in the internal mechanism of the algorithm, the structure used, and the operations employed in some of the commonly used hash functions is provided. In Table 3, information about the types and complexities of attacks against these algorithms is presented (Maetouq etc al., 2018).

Table 6. A General Features Table of Some Common Hash Algorithms

Properties	Name Of Algorithm				
	MD5	RIPEMD-160	SHA-1	SHA-2 256/512	SHA-3 256/512
Block Size (Bits)	512	512	512	512/1024	1088/576
Word Size (Bits)	32	32	32	32/64	320/320
Output Size (Bits)	128	160	160	256/512	1600/1600
Rounds	18	80	80	64/80	24/24
Operations	Xor,Or, And,Not, Add,Shift	Xor,Or, And,Not, Add,Rotate	Xor,Or, And,Not, Add,Rotate	Xor,Or, And,Shift, Add,Rotate	-
Construction	Merkle-Damgard	Merkle-Damgard	Merkle-Damgard	Merkle-Damgard	Sponge

Source : (Maetouq etc al., 2018)

Table 7. Types of attacks and their complexity on common hash functions

Algorithm	Type of attacks	Complexity
MD5	Collision	2^{39}
	Fast Collision	2^{18}
RIPEM-160	Collision	2^{67}
	Preimage	$2^{158.91}$
SHA-1	Collision	$<2^{69}$
	Collision	2^{61}
	Freestart Collision	-

SHA-2/256	Preimage	$2^{255.5}$
SHA-2/512	Preimage	$2^{511.2}$
SHA-3/256	Practical Collision and near-Collision	-
SHA-3/512	Possibility first collision	-

Source : (Maetouq etc al., 2018)

Table 8. Hashing Algorithms for Multi-Label Image Retrieval

Approach	Transfer Learning	Network Architecture
Pointwise		
Direct binary embedding	No	ResNet50
Deep multi-label hashing	-	AlexNet
Multi-task deep hashing	Yes	GoogLeNet
Discriminative cross-view hashing	No	ResNet50
Pairwise		
Multi-label supervised deep hashing	Yes	Generic CNN
Deep multilevel semantic similarity preserving hashing	No	AlexNet
Deep multi-similarity hashing	No	Generic CNN
Instance similarity deep hashing	Yes	AlexNet
Deep uniqueness-aware hashing	No	AlexNet
Tripletwise		
Instance-aware hashing	Yes	GoogLeNet
Triplet-based deep binary embedding	Yes	VGG-16
Hashing for multi-labeled data	-	VGG
Deep supervised hashing with code operation	Yes	VGG and ResNet
Listwise		
Deep semantic ranking based hashing	Yes	AlexNet

Approach	Transfer Learning	Network Architecture
Order-sensitive deep hashing	No	AlexNet
Object-location-aware hashing (Huan	-	GoogLeNet
Rank-consistency deep hashing	Yes	VGG

Source: (Rodrigues, Cristo & Colonna, 2020)

Supervised methods are among the most commonly used approaches for classifying the hashes of similar images with Deep Hashing. Some of the supervised methods found in the literature are presented in Table 4. The methods are categorized into four main groups: pointwise, pairwise, tripletwise, and listwise. These methods are used in multi-label image retrieval problems.

9. Supervised Methods

9.1 Pointwise Method

In this method, the correspondence between class labels and images in the dataset is used to teach which class the image belongs to.

9.2 Pairwise Method

In this method, the images in the dataset are taken in pairs. The neural network learns whether the image pairs are similar or not and stores the obtained information in the Hamming space.

9.3 Tripletwise Method

In this method, the neural network takes three images from the dataset as input. One of these images is referred to as q. It is taught that the image q is more similar to one of the other two images. This way, the hash codes of similar images are brought closer to each other.

9.4 Listwise Method

In this method, one of the images in the dataset is designated as the query. Along with the query image, a list is created by ranking a set of images based on their similarity to the query image. In this way, the images are obtained in order from least similar to most similar to the query image (Rodrigues, Cristo & Colonna, 2020).

10. Conclusion

Hash functions are widely used in various cryptographic applications such as data integrity verification, digital signatures, blockchain, and authentication. The widespread use of hash functions in many applications stems from their ability to convert an original input of arbitrary length into a fixed and very short length in a one-way manner. The output of the hash function is irreversible. This feature makes hash functions unique and indispensable in many cryptographic fields.

Hash functions have entered a progressively evolving and diversifying process as traditional hash functions, AI-supported hash functions, and quantum hash functions. All efforts in this process aim to design hash functions that are more resistant to attacks, more secure, and more functional by relying on the original data.

It can be said that future trends will focus on the development of AI-supported hash functions and quantum hash functions. It is suggested that hash codes generated with AI support will be more compatible with the original data and more secure. The recent trend in studies in the field of artificial intelligence will encourage more researchers to focus on AI-supported hash function designs. Additionally, the fact that quantum computers can perform cryptographic operations much faster than traditional computers indicates that quantum hash applications will be among the trending studies in the future.

In this book chapter, by considering the transformation process of hash functions, information is provided about the types of hash functions, their working principles, the security features they offer, their areas of use, new trends, and future studies, offering readers a comprehensive perspective on hash functions.

RESORCES

Naidu, J. L., Gorakala, A. C., & Amiripalli, S. S. (2020). Hash functions and its security for Snags. IRJET, 7(7), 3465-3471.

Akoto-Adjepong, V., Okyere-Gyamfi, S., & Asante, M. (2020). An Enhanced Non-Cryptographic Hash Function.

Zellagui, A., Hadj-Said, N., & Ali-Pacha, A. (2019, April). Comparative Study Between Merkle-Damgård And Other Alternative Hashes Construction. In Proceedings of the Second Conference on Informatics and Applied Mathematics IAM, Guelma, Algeria (pp. 24-25).

Debnath, S., Chattopadhyay, A., & Dutta, S. (2017, November). Brief review on journey of secured hash algorithms. In 2017 4th International Conference on Opto-Electronics and Applied Optics (Optronix) (pp. 1-5). IEEE.

De Canniere, C., Biryukov, A., & Preneel, B. (2006). An introduction to block cipher cryptanalysis. Proceedings of the IEEE, 94(2), 346-356.

Wijitrisnanto, F., & Susanti, B. H. (2018, November). Faster multicollision attack on Davies-Meyer hash function scheme implementing Simeck32/64 block cipher algorithm. In IOP Conference Series: Materials Science and Engineering (Vol. 453, No. 1, p. 012011). IOP Publishing.

Al-Odat, Z., & Khan, S. (2019, December). Constructions and attacks on hash functions. In 2019 International Conference on Computational Science and Computational Intelligence (CSCI) (pp. 139-144). IEEE.

Zellagui, A., Hadj-Said, N., & Ali-Pacha, A. (2019, April). Comparative Study Between Merkle-Damgård And Other Alternative Hashes Construction. In Proceedings of the Second Conference on Informatics and Applied Mathematics IAM, Guelma, Algeria (pp. 24-25).

Kumar, A., Gupta, D. N., & Kumar, R. (2021, October). Hash Constructions for CoAP under an IoT Environment. In 2021 International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON) (pp. 1-7). IEEE.

Maetouq, A., Daud, S. M., Ahmad, N. A., Maarop, N., Sjarif, N. N. A., & Abas, H. (2018). Comparison of hash function algorithms against attacks: A review. International Journal of Advanced Computer Science and Applications, 9(8).

Ali, A. M., & Farhan, A. K. (2020). A novel improvement with an effective expansion to enhance the MD5 hash function for verification of a secure E-document. IEEE Access, 8, 80290-80304.

Khan, B. U. I., Olanrewaju, R. F., Morshidi, M. A., Mir, R. N., Kiah, M. L. B. M., & Khan, A. M. (2022). Evolution and Analysis Of Secure Hash Algorithm (Sha) Family. Malaysian Journal of Computer Science, 35(3), 179-200.

Al-Odat, Z., Abbas, A., & Khan, S. U. (2019, December). Randomness analyses of the secure hash algorithms, SHA-1, SHA-2 and modified SHA. In 2019 International Conference on Frontiers of Information Technology (FIT) (pp. 316-3165). IEEE.

Guitouni, Z., Ammar, N., & Machhout, M. (2024). An efficient hardware implementation of SHA-3 using 3D cellular automata for secure blockchain-based IoT systems. Engineering Research Express, 6(4), 045212.

Sharma, J., & Koppad, D. (2016, December). Low power and pipelined secure hashing algorithm-3 (SHA-3). In 2016 IEEE Annual India Conference (INDICON) (pp. 1-5). IEEE.

Kuila, S., Chawdhury, D., & Pal, M. (2015). On the SHA-3 hash algorithms. J. Math. Inform, 3, 2349-0632.

Dolmeta, A., Martina, M., & Masera, G. (2023). Comparative study of Keccak SHA-3 implementations. Cryptography, 7(4), 60.

Sadeghi-Nasab, A., & Rafe, V. (2023). A comprehensive review of the security flaws of hashing algorithms. Journal of Computer Virology and Hacking Techniques, 19(2), 287-302.

Tajane, K., Pitale, R., Zambre, S., Huda, H., Utage, A., & Dhar, V. (2024, May). Efficient Cloud Data Deduplication with Blake3 and Secure Transfer using AES. In 2024 4th International Conference on Pervasive Computing and Social Networking (ICPCSN) (pp. 572-579). IEEE.

Biryukov, A., Dinu, D., & Khovratovich, D. (2016, March). Argon2: new generation of memory-hard functions for password hashing and other applications. In 2016 IEEE European Symposium on Security and Privacy (EuroS&P) (pp. 292-302). IEEE.

Cao, W., Feng, W., Lin, Q., Cao, G., & He, Z. (2020). A review of hashing methods for multimodal retrieval. IEEE Access, 8, 15377-15391.

Singh, A., & Gupta, S. (2022). Learning to hash: a comprehensive survey of deep learning-based hashing methods. Knowledge and Information Systems, 64(10), 2565-2597.

Hatanaka, T., Fushio, R., Watanabe, M., Munro, W. J., Ikeda, T. N., & Sugiura, S. (2024). A Quantum-Resistant Photonic Hash Function. arXiv preprint arXiv:2409.19932.

Ablayev, F., & Vasiliev, A. (2013). Quantum hashing. arXiv preprint arXiv:1310.4922.

Upadhyay, D., Gaikwad, N., Zaman, M., & Sampalli, S. (2022). Investigating the avalanche effect of various cryptographically secure Hash functions and Hash-based applications. IEEE Access, 10, 112472-112486.

Genç, Y., & Afacan, E. (2021, April). Design and implementation of an efficient elliptic curve digital signature algorithm (ECDSA). In 2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS) (pp. 1-6). IEEE.

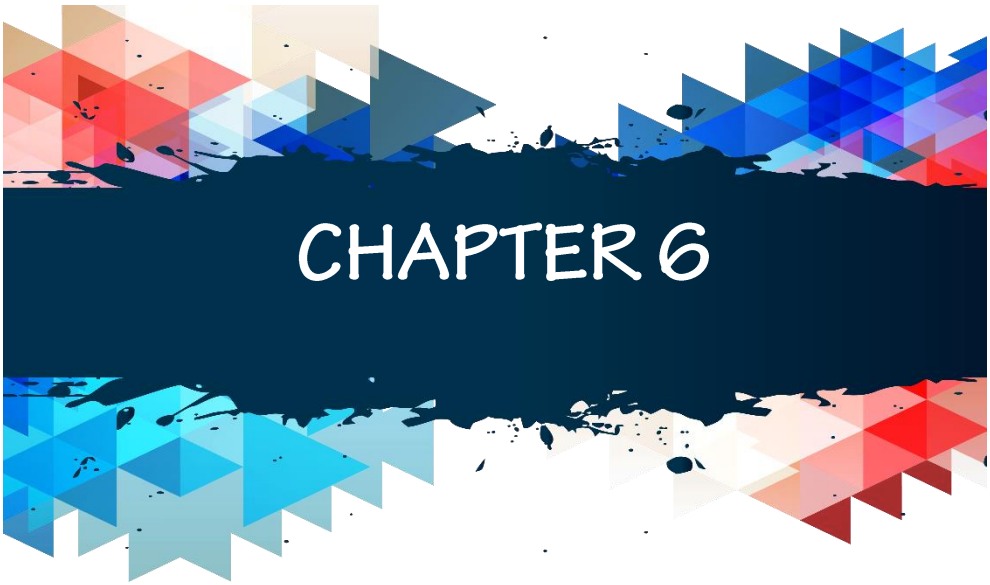
Sadeghi-Nasab, A., & Rafe, V. (2023). A comprehensive review of the security flaws of hashing algorithms. Journal of Computer Virology and Hacking Techniques, 19(2), 287-302.

Martino, R., & Cilardo, A. (2019). A flexible framework for exploring, evaluating, and comparing SHA-2 designs. IEEE Access, 7, 72443-72456.

Gunathilake, N. A., Al-Dubai, A., & Buchana, W. J. (2020, November). Recent advances and trends in lightweight cryptography for IoT security. In 2020 16th International Conference on Network and Service Management (CNSM) (pp. 1-5). IEEE.

Maetouq, A., Daud, S. M., Ahmad, N. A., Maarop, N., Sjarif, N. N. A., & Abas, H. (2018). Comparison of hash function algorithms against attacks: A review. International Journal of Advanced Computer Science and Applications, 9(8).

Rodrigues, J., Cristo, M., & Colonna, J. G. (2020). Deep hashing for multi-label image retrieval: a survey. Artificial Intelligence Review, 53(7), 5261-5307.



Network Security and Applications within the scope of Information Security Management

Harun Şeker[1,2] & Vedat Marttin[3]

[1] BG-TEK Information Security Technologies, Bursa- Türkiye
[2], Bilecik Seyh Edebali University, Institute of Graduate Education, Computer Engineering-MD, TR, 11100 Bilecik - Türkiye.ORCID: 0000-0002-9205-4035
[3] Asst. Prof., Bilecik Seyh Edebali University, Computer Engineering Department,TR, 11100 Bilecik - Türkiye. ORCID: 0000-0001-5173-2349, Corresponding author

1. Introduction

Information Security Management System (ISMS) aims to protect data by ensuring confidentiality, integrity and availability. These principles form the core of ISMS, which is implemented through the PDCA (Plan-Do-Check-Act) cycle to facilitate continuous improvement. This process includes creating policies and procedures, implementing and managing controls, monitoring performance and taking corrective actions when necessary. To ensure network security, organizations should create an asset inventory to identify critical resources, conduct risk assessments to assess potential threats and vulnerabilities, define access matrices to regulate user permissions and create security policies tailored to organizational needs. These policies emphasize the importance of a systematic, policy-oriented approach to prevent inefficiencies and minimize operational costs by covering key areas such as access control, password complexity, encryption and event monitoring. It explains network security systems and techniques in detail.

In the study, after the literature review, the importance and steps of ISMS are given in order. Then, firewalls, proxy servers and content filters, intrusion detection and prevention systems, network segmentation, virtual networks, NAC (Network Access Control) applications, VPN (Virtual Private Network), network monitoring and updating are explained in detail and information is given about penetration testing and vulnerability scanning processes.

In literatur, Fırlar (2003) addressed the security problems in IP networks and proposed a mechanism to solve these problems. In the study, the concept of network security was examined in detail and security problems in Internet, Ethernet and IP networks were analyzed. In particular, different security models for protecting data and resources on the network were defined and the functions of firewalls were detailed. Strategies and methods that can be used for network security were examined (Fırlar T., 2003).

Tekerek (2008) emphasized in his study that information security management should be considered as a dynamic process. It was stated that information security cannot be provided only with technical measures, and administrative measures, standards (such as ISO 27001) and the human factor should also be integrated into the process. The study draws attention to the importance of institutional policies, risk management and awareness training for ensuring information security (Tekerek M., 2008).

Can and Akbaş (2014) discussed the importance of corporate network and system security policies and a case study on the creation and implementation of these policies. The study emphasized that security policies play a critical role in

ensuring the information security of institutions. It was stated that network and system security policies should be comprehensive not only against external threats but also against threats that may come from within the institution. In addition, the importance of regular trainings as well as tools such as firewall, intrusion detection systems and anti-virus to reduce security threats was emphasized (Can & Akbaş ,2014).

Kumar and Malhotra (2015), in their study on network security threat models and protection methods, detailed various types of cyber attacks and the precautions that can be taken against these attacks. In the study, protection models such as firewall and intrusion detection systems were proposed against threats. They presented innovative algorithms and tools for the detection and solution of firewall rule anomalies. The effectiveness of these methods in eliminating security vulnerabilities and ensuring data security was emphasized (Kumar & Malhotra, 2015).

Coulibaly (2020) comprehensively examined Intrusion Detection Systems (IDS) used to detect attacks and Intrusion Prevention Systems (IPS) that serve both detection and prevention purposes. In addition, the applications of machine learning techniques in these systems and their effects on improving performance were evaluated. The limitations of IDS and IPS systems were highlighted, and the effectiveness of hybrid systems and machine learning integrations in reducing these limitations was highlighted (Coulibaly K., 2020).

In their study, Liang and Kim (2022) examined the evolution of firewalls and the importance of next-generation firewalls (NGFW) for the purpose of improving network security. The study discussed the development process from the first generation packet filtering firewalls to NGFW and the advantages offered by these systems. It was emphasized that NGFW offers advanced features such as higher performance, deep packet inspection (DPI) and intrusion detection/prevention systems (IDS/IPS) compared to traditional firewalls. The study shows that NGFW provides a more secure environment in industrial and corporate networks with its multi-layered security approach(Liang & Kim , 2022).

Li et al. (2014) discussed the evaluation and implementation of network access control (NAC) technologies. The study provides technical analysis of technologies such as IEEE 802.1x, Trusted Network Connection (TNC), and Network Access Protection (NAP). In addition, the design of network access control systems, policies, and policy implementation are discussed. The study emphasizes that openness, compatibility, and standardization play a critical role in network access control systems(Li et al., 2014).

Mehdizadeh et al. (2017) examined the effects of Virtual Local Area Networks (VLANs) on network segmentation and security. The study highlighted the advantages of VLANs in optimizing network traffic, reducing costs, and increasing security. It was also stated that VLANs allow network administrators to provide user and port control by dividing a physical network into logical segments. The study addressed the protection methods of VLANs against threats such as ARP attacks and VLAN hopping. As a result, it was stated that VLANs play a critical role in network management and security in terms of scalability, security, cost, and efficiency (Mehdizadeh et al., 2017).

Nourildean et al. (2023) investigated ad-hoc routing protocols to improve VLAN performance in wireless networks. The study highlights the benefits of VLAN technology, such as increasing network efficiency, managing traffic, and improving security. However, it was stated that VLANs have disadvantages such as low data transfer speed while reducing network transition delays. The study aimed to improve VLAN performance, especially latency and data transfer speed, by using ad-hoc routing protocols. Tests conducted with the Riverbed Modeler simulation tool showed that these protocols significantly improved network performance, providing low latency and high data transfer speed (Nourildean et al., 2023).

Makeri et al. (2021) examined the improvement of enterprise network performance using VLAN. The study aimed to optimize existing network structures with VLAN technology and increase network performance parameters such as security, speed, and bandwidth utilization. The study underlined the advantages of VLAN applications such as traffic segmentation, control of broadcast domains, and ease of management. It was found that VLAN technology increases security in the network, reduces management costs, and provides more efficient resource utilization. The study also showed that the performance limitations of traditional network designs can be overcome with the use of VLAN (Makeri et al., 2021).

Alshalan et al. (2016) examined mobile VPN technologies in detail and evaluated their main features, advantages, and challenges. The study emphasized that traditional VPN solutions often fail due to intermittent connections in the mobile environment, while Mobile VPNs maintain connection continuity by adapting to network changes. Various mobile VPN protocols (IPsec, TLS, etc.) and technologies were compared, and their strengths and weaknesses in terms of performance, security, and connection continuity were analyzed (Alshalan et al., 2016).

In his study, Solisch (2022) examined VPN technologies and evaluated the architectures, purposes of use, and advantages of different VPN solutions. In the

study, VPNs were classified according to the layers in the OSI model, and L2VPN and L3VPN solutions were particularly focused on. It was stated that L2VPN technology creates Ethernet-based connections by providing data connectivity between customer devices, while L3VPN improves network routing functionality. The comparison of tunneling protocols such as IPsec and GRE in terms of security and performance also constituted an important part of the study. As a result, it was emphasized that the selection of VPN technology and the determination of the tunneling protocol vary depending on the application context (Solisch T., 2022).

González-Granadillo et al. (2021) comprehensively examined the current status of Security Information and Event Management (SIEM) systems and their use in critical infrastructures. SIEM solutions are used to manage and report threats in security operations centers (SOCs) by collecting, analyzing, and correlating events from a wide variety of sources. The study analyzed the strengths and weaknesses of existing SIEM systems and emphasized the central role played by SIEM systems in preventing, detecting, and responding to cyberattacks(González-Granadillo et al., 2021).

In their study, Arfeen et al. (2021) examined endpoint detection and response systems (EDR) in cybersecurity in detail and evaluated the capabilities of these systems to detect, prevent and respond to malware. It was emphasized that EDR systems offer an integrated solution with continuous monitoring, threat detection, event analysis and automatic response features, and it was stated that they provide faster and more effective threat management by combining network and endpoint data, and also produce fewer false positive results compared to traditional security tools. It was stated that EDR systems reduce the workload for the SOC and can respond to cyber threats faster. It was emphasized that EDR solutions should be better integrated with machine learning and artificial intelligence for future threats (Arfeen et al., 2021).

Karantzas and Patsakis (2021) evaluated the effectiveness of Endpoint Detection and Response (EDR) systems in combating Advanced Persistent Threats (APT). The study simulated various APT attack vectors and examined the performance of 11 modern EDR systems in detecting and blocking these threats. The findings reveal that EDR systems fail to detect many attacks and reveal vulnerabilities. In particular, it was stated that situations such as DLL loading and missing low-priority alerts can slow down the responses of security teams. The study emphasizes the need to use machine learning and artificial intelligence to improve the detection mechanisms of EDR systems (Karantzas & Patsakis , 2021)

Islam, et al. (2020) systematically examined various dimensions of security orchestration, evaluated existing solutions, and identified future research areas. The study defined the concept of security orchestration, which enables different security tools to be integrated and collaborate effectively, and detailed the basic functions of this technology, such as automation and process management. The study examined the level of technical requirements of existing security orchestration systems, such as flexibility, scalability, and interoperability, and discussed open research topics in this area (Islam, et al., 2020).

In his study, Vegesna (2022) emphasized that vulnerability scanning and penetration testing applications can be used as an effective method to prevent cyber attacks. In the study, the entire life cycle of vulnerability scanning and penetration testing processes was defined and the stages of vulnerability scanning and penetration testing were detailed. While vulnerability scanning focuses on detecting vulnerabilities in the system, penetration testing allows the analysis of the weak points of the system by authoritatively exploiting these vulnerabilities. The study also discussed vulnerability scanning and penetration testing techniques and listed 15 commercial and open source tools used in these processes. It was concluded that vulnerability scanning and penetration testing were effective in providing proactive defense and reducing the effects of cyber attacks (Vegesna V.V.,2022).

2. Information Security Management System

Information security is a crucial aspect of protecting data in modern physical and digital environments. Since information can exist in various forms—such as written on paper, stored electronically, transmitted via email or physical mail, or shared verbally—it requires appropriate measures to ensure its protection. The foundation of information security lies in maintaining the confidentiality, integrity, and availability of information.

Confidentiality, ensuring that information is not accessed or disclosed to unauthorized individuals. Protects sensitive data, such as personal information and trade secrets, from unauthorized exposure.For Instance, encryption, authentication, and access control mechanisms.

Integrity,preserving the accuracy and consistency of information by preventing unauthorized modifications.Ensures that data remains trustworthy and unaltered unless explicitly authorized. For example,data integrity checks, digital signatures, and hash algorithms.

Availability,ensuring that authorized users can access information when needed, even in the face of potential disruptions. Supports the continuity of critical

operations and business processes. For Instance, backup systems, disaster recovery plans, and robust network security (Marttin & Pehlivan, 2010).

These principles work together to form the backbone of information security management. Each principle addresses specific types of threats, and their balanced implementation creates a secure information environment. Figure 1 shows the PDCA Cycle for Network Security.

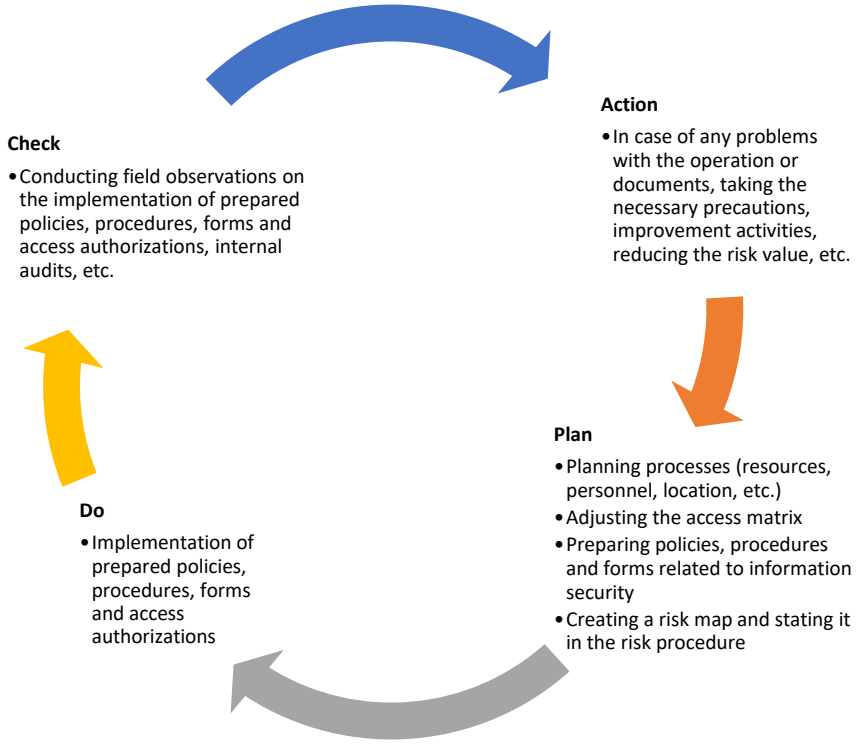


Figure 1: PDCA Cycle for Network Security

Plan, this step involves developing the Information Security Management System (ISMS) policy, objectives, targets, processes, and procedures.

Do, at this stage, the ISMS policy, controls, processes, and procedures are implemented and put into operation.

Check,this phase focuses on assessing the performance of ISMS policies, objectives, and processes. Where applicable, measurements are taken, and the results are reported.

Act, based on the outcomes of management reviews, corrective and preventive actions are carried out to maintain and enhance the ISMS.

Information security management should be seen as an ongoing process of continuous improvement. It operates within a cycle, as outlined by the PDCA (Plan-Do-Check-Act) model, and never ceases.

The PDCA model, in summary, is about deciding what actions need to be taken, implementing those decisions, verifying that they are working as intended, and taking measures to address any controls that do not meet the desired objectives.

In order to ensure network security, it is first necessary to identify the assets that need to be protected and to determine which assets need to be protected from which threats and in what way (Tekerek M., 2008).

2.1. Creating an Asset Inventory

In order to ensure security, a comprehensive analysis should be conducted to create an asset inventory and to determine which assets are available (ISO/IEC 27001:2022a).

An asset inventory is a detailed list that includes everything that is valuable to the organization and needs to be protected, such as hardware, software, and data assets. An asset inventory can be created using methods such as surveys, face-to-face interviews, documentation review, and automatic scanning tools.

These assets and sensitive data types are identified and categorized. Ownership and responsibilities are determined for each asset. This process forms the basis for identifying vulnerabilities and threats (ISO/IEC 27001:2022a).

2.2. Risk Analysis

After the inventory is created, a risk analysis should be performed to evaluate possible threats and vulnerabilities(ISO/IEC 27001:2022b).Cyber attacks, malware, human errors, natural disasters and similar threats that may affect assets are taken into consideration. Security vulnerabilities are compared with existing measures to determine the risk level. The obtained risks are used to shape security policies.

2.3. Creating an Access Matrix

It is created to determine the access levels of users to assets. Users are classified according to their duties and authorizations, and it is determined which assets

they can access with which authorizations (read, write, change). User access rights are defined and permissions are prevented (ISO/IEC 27001:2022c).

2.4. Creating Security Policies

After determining which users will access which assets with which authorizations through applications such as asset inventory, risk analysis and access matrix, security policies appropriate to the needs should be created (Can & Akbaş, 2014). Security policies are principles, rules and guidelines prepared and adopted to protect information assets. They consist of accepted risk tolerance, controls and procedures to be applied. Security policies cover issues such as network access permissions, network access methods, password complexity and encryption requirements, and event monitoring procedures (Astrida, et.al, 2016). Measures to be taken for network security must be based on a policy. The effectiveness of randomly taken measures is open to discussion and can be costly.

3. Firewalls

They are hardware or software that provides or prevents communication between networks according to certain rules. They can be divided into two groups as host-based and network-based depending on where they work (Mukkamala & Rajendran, 2020),(Vacca, J. R., 2024a)

3.1. Host-Based Firewalls

They are software-based firewall applications that run on a computer system. They check and accept packets coming and going to a computer system and only provide security for the computer system they work on (Vacca, J. R., 2024b).

Firewall software that comes integrated into operating systems or personal firewall software that can be installed later can be considered in this category.

3.2. Network Firewalls

They are firewalls that protect systems in a network segment and are responsible for border security. Such firewalls can be thought of as routers that decide whether packets will pass to another network segment by looking at a list of rules (Vacca, J. R., 2024b).

They usually consist of a Unix-type operating system running on hardware with many network interfaces. They can include different features such as packet filtering, NAT (Network Address Translation), Content Filtering, VPN.

Firewalls can be divided into 4 categories according to their working methods: Static Packet Filtering, Stateful Packet Filtering, Application Layer (Layer 7) Filtering and Hybrid Filtering.

3.2.1. Static Packet Filtering

Static packet filtering is a firewall that provides access control based on protocol header information such as source IP address, destination IP address, source port, destination port and protocol type. Such firewalls manage data traffic between networks by referring to the Access Control List (ACL) defined by the system administrator (Cheswick et.al, 2003),(Zhang & Wang, 2021).

Since filtering is done by looking only at protocol header information, it cannot perform data analysis that occurs at higher layers. This limitation may allow attackers to bypass the firewall by imitating an existing connection and access systems in the background or scan the network through various TCP/IP manipulations.

Static packet filtering has low resource usage and high filtering speed due to its simplicity. Thanks to these features, it offers an effective solution especially in cases where detailed data examination is unnecessary and in backbone systems with high-speed network connections. It is also a suitable method to meet basic security requirements in low-capacity hardware.

3.2.2. Stateful Packet Filtering

Network connections consist of a start, data transfer and end phases. Stateful firewalls have a structure that tracks the stages of these connections (Vacca, J. R., 2024a), (Klein, A., 2021). It continuously monitors when and from which source each connection starts, which destination it is directed, the protocols and ports used, the status of the connection (e.g., SYN_WAIT, ESTABLISHED) and whether it is active or not. After the connection is started, the necessary rules are automatically created to accept return packets and packets belonging to connections not included in the rule table are blocked (Figure 2).

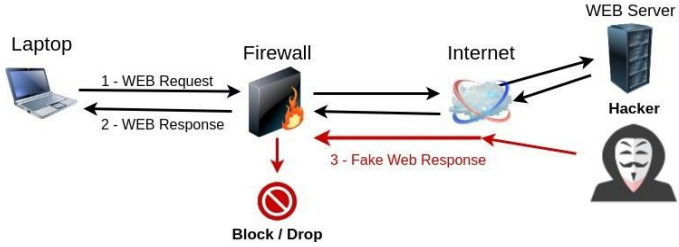


Figure 2: Stateful Firewall Diagram

It provides a more advanced protection mechanism thanks to state monitoring. Packets that do not belong to the connection or originate from fake connections are blocked. In addition, attackers who try to bypass the firewall with various TCP/IP manipulations can be prevented from sending packets to systems or scanning ports with this method.

State-controlled firewalls require more system resources such as CPU and memory (RAM) because they write and read data to the state table for each packet. For example, OpenBSD Packet Filter, an open source firewall, keeps two state records for each connection and requires approximately 1 KB of memory space to keep each record [29]. Considering that 500,000 simultaneous connections will create 1,000,000 records in the state table, approximately 976 MB of free memory space will be needed. If the state table fills up or the system memory runs out, the firewall will not be able to accept new connections and will lose its functionality.

Stateful firewalls are preferred in large and complex network structures where there are no resource constraints, high security requirements, and where a large number of connections and sessions must be constantly monitored.

3.2.3. Application Layer (Layer 7) Packet Filtering

Firewalls operating at the application layer operate at the application layer, which is the seventh layer of the OSI model. These firewalls try to detect certain patterns by looking at the data segments of application protocols such as HTTP and FTP, as well as the protocol header information of transmitted packets, and accordingly decide whether to allow the packets to pass or not (Vacca, J. R., 2024a).Application layer firewalls can recognize various protocols, block certain applications, detect malicious traffic, and capture patterns of attacks coming from this layer (Cheswick et.al, 2003).

These firewalls require a significant amount of system resources as they perform numerous scans and inspections on the content of each packet. Therefore, the processing times of packets are longer compared to other filtering methods, which can cause performance loss.

However, they cannot directly access the data carried in encrypted traffic such as SSL/TLS. Therefore, it is not possible to detect the patterns sought in encrypted protocols such as HTTPS, and this limits the effectiveness of the filtering method. A type of Man-in-the-Middle method can be applied to decrypt the encrypted traffic between the client and the server, and the decryption process can be performed. However, this process requires more system resource usage and creates an additional load on performance, as it includes both decryption and

re-encryption processes. In addition, the application of this method may not always be effective, as it can lead to SSL/TLS errors on clients.

This type of filtering is generally known as Deep Packet Inspection (DPI) and is preferred in critical network infrastructures that require high security and do not have resource constraints.

3.2.4. Hybrid Filtering

Hybrid filtering refers to firewalls that apply more than one filtering method simultaneously. Such firewalls provide more comprehensive protection by integrating different filtering techniques. Many leading firewalls today have the ability to use one or more of several approaches, such as static packet filtering, stateful filtering, and application layer filtering. In this way, both flexibility is provided and security needs can be met from a broader perspective.

4. Proxy Servers and Content Filters

Proxy servers are intermediate systems that indirectly provide access to the Internet for clients on the network. These servers allow clients to benefit from websites, while preventing them from connecting directly to the Internet. When a client notifies the proxy server of the website they want to access, the proxy server downloads the relevant content from the original website and forwards it to the client (Vacca, J. R., 2024a). Thanks to this mechanism, clients are isolated from external networks without communicating directly with them (Figure 3).

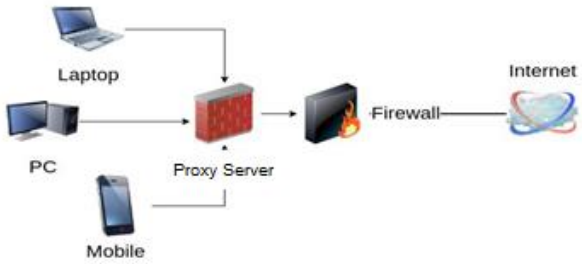


Figure 3: Web Proxy

A significant advantage of this application is that the requests made by the clients can be recorded, controlled and access to unwanted websites can be blocked. Instead of defining a proxy server for the clients, HTTP(S) traffic can be directed to the proxy server by applying NAT at the network layer. This method is called "Transparent Proxy Server" (Wessels D.,2004).

5. Intrusion Detection and Prevention Systems

Intrusion detection systems (IDS) work passively, generating warnings about potential attacks and recording these attacks. In contrast, intrusion prevention systems (IPS) can play a more active role against potential threats, blocking dangerous traffic and terminating malicious connections (Vacca, J. R., 2024c). Intrusion detection and prevention systems are generally based on two main methods: signature-based and anomaly-based (Marttin & İmal, 2015). While signature-based systems detect threats by scanning network traffic for predetermined attack signatures for known threats, anomaly-based systems identify potential attacks by identifying unusual activities on the network. In order for anomaly-based systems to be effective, they must learn the normal flow of the network by monitoring the normal activities of the network for a certain period of time and creating a statistical model (Marttin, V.,2014).

6. Network Segmentation and Virtual Networks

Network segmentation is the process of dividing a network into smaller and isolated sections, either logically or physically. Data traffic between these sections should be controlled and communication should only be provided between the specified segments (ISO/IEC 27001:2022d). The main purpose of segmentation is to facilitate network management processes, increase security and reduce the attack surface (Vacca, J. R., 2024d).

The corporate network can be divided into physical or virtual components according to the needs. Communication between these components should be provided based on the principle of least privilege and access to segments that do not need to communicate should be restricted.

6.1. Physical Segmentation

Physical segmentation refers to the separation of a network into separate physical sections using network devices such as routers and switches (Vacca, J. R., 2024e). For example, the production network, office network, and guest network are physically isolated by being managed through separate hardware.

6.2. Logical Segmentation

Logical segmentation is the division of a network into virtual sections using technologies such as VLANs, despite the physical presence of a single network. This type of segmentation increases the security and manageability of the network by creating isolated virtual networks between devices that share the same physical network hardware.

6.3. VLAN (Virtual Local Area Network)

VLAN refers to logical networks defined virtually on physical network devices (Institute of Electrical and Electronics Engineers, 2022) and is defined by the IEEE 802.11Q standard. A VLAN separates network traffic into specific groups and allows only these groups to communicate with each other (Tarlacı et al.,2019). These virtual networks can be managed effectively thanks to configuration changes made on smart switching devices and routers.

For example, by defining separate VLANs for the IT department, accounting department and guest network in an institution, data traffic between these departments can be controlled. This application is important in terms of increasing network security and facilitating management processes.

6.4. Safe Zone (DMZ- Demilitarized Zone)

DMZ is a buffer zone where servers hosting public services such as web servers and e-mail servers are isolated from the internal network and the Internet (Vacca, J. R., 2024f). Servers within this area are separated from both the internal network and the Internet by firewalls (Figure 4). In case of possible attacks from outside, even if these isolated servers are compromised, direct access to the internal network by attackers can be prevented. Thus, the security of the internal network is increased.

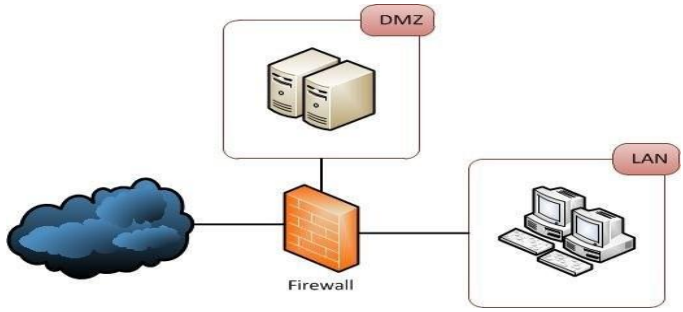


Figure 4: DMZ Diagram

6.5. Guest Networks

Guest networks are networks that are specifically reserved for visitors, independent of the corporate network. These networks are completely isolated from the main network and provide only limited internet access (Figure 5). In order for guests to access the internet, they usually need to log in with a guest account (Viecco C.,2013a). In some guest networks, users can register to the network by verifying their ID number and GSM number (TBMM, Law No:5651, 2007),(BTK, 2013). This structure contributes to the protection of the internal network against security breaches that may be caused by visitors, while facilitating the identification of the perpetrator in cybercrimes that may be committed over the corporate internet connection.

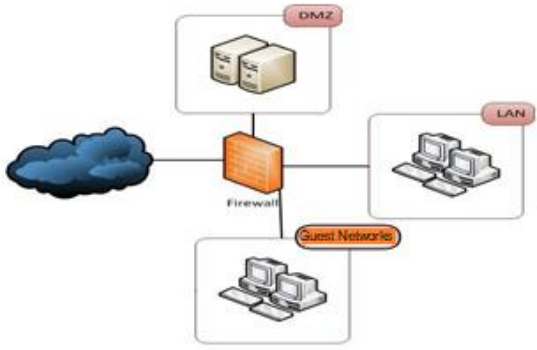


Figure 5: Guest Network Diagram

7. NAC (Network Access Control) Applications

NAC applications are an 802.1x-based security mechanism that manages the authentication, authorization, and access control processes of clients that join the network (Viecco C.,2013b), (Vacca, J. R., 2024g). This mechanism is critical for increasing network security and preventing unauthorized access. NAC applications are widely used, especially in corporate networks, to reduce security breaches and ensure data integrity.

7.1. Authentication Process

The IEEE 802.1x standard forms the basis of NAC applications. This protocol requires a client to authenticate before connecting to the network. When a client requests to connect to the network, it transmits its credentials (usually a username and password) to an authentication server. The authentication server authenticates the client, grants access to the network, and the client is granted access to the network; otherwise, access is denied.

7.2. Access Control and Policy Management

NAC applications also manage access control policies. These policies determine the access permissions of users and devices to the network. For example, when an employee connects to the network, their authorization is verified and only authorized resources are accessed. Additionally, guest or temporary users are hosted in isolated subnets, increasing the security of the main network.

7.3. Use of Isolated Subnets

In some network structures, clients connecting to the network are first directed to an isolated subnet environment. This subnet is designed only for the authentication process. When the user provides the correct credentials, the system transfers the user to the real network segment. This application protects the integrity of the network by minimizing potential security threats.

7.4. Device Detection and Management

NAC systems use advanced detection mechanisms to identify and classify devices connected to the network. In this way, only devices with secure and up-to-date software are allowed to access the network. NAC applications also perform critical functions such as threat detection, management of security vulnerabilities, and implementation of security policy.

8. VPN (Virtual Private Network)

A VPN (Virtual Private Network) is conceptually defined as a type of connection in which network traffic between two points is passed through an encrypted tunnel (Vacca, J. R., 2024k). This encrypted tunnel can be thought of as a structure that connects two computer systems with a virtual cable. VPN networks provide a high level of security by encrypting each data packet transmitted through tunneling protocols (Klein, A., 2021). Even if an attacker tries to listen in on VPN traffic, they cannot make sense of the data packets because they do not have the tunnel encryption keys. Therefore, VPN technology is critical for connecting networks securely over the Internet.

VPN connections are generally examined in two main categories: "site-to-site" VPN connections, which connect different networks, and "client-to-site" (remote access) VPN connections, which allow a client to connect to a local network over the internet.

8.1. Site-to-Site VPN

Site-to-site VPN connections are typically used to securely communicate across large networks that are geographically dispersed (Figure 6). In this type of connection, the local networks included in the VPN form a single, large network.

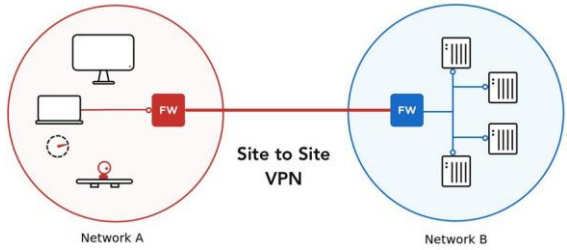


Figure 6: Site to Site VPN Diagram

8.2. Client-to-Site VPN

Client-to-site VPN allows a computer located outside the network to join the local network securely (Figure 7). With this method, users working outside the office gain access to local network resources through an encrypted tunnel. The VPN software running on the client side establishes an encrypted tunnel by communicating with the VPN terminator (e.g. firewall) on the network side. Network traffic is passed through this tunnel and the client is securely connected to the local network. If necessary, all of the client's internet traffic can be routed through this tunnel, providing internet access as if it were a client on the local network.

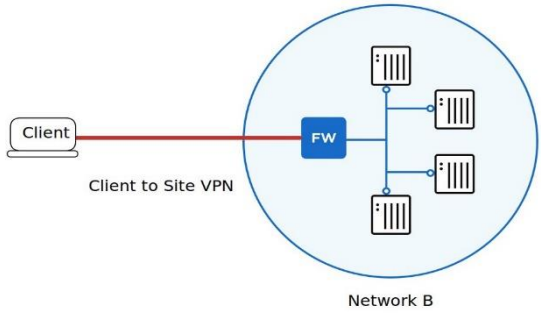


Figure 7: Client to Site VPN Diagram

8.3 VPN Technologies

There are various technologies used for VPN. These technologies provide basic functions such as tunneling (encapsulation), encryption and authentication.

Tunneling is a process performed by adding new headers to the headers of packets carrying data. In this process, the routers through which the packet passes only act in accordance with the newly added headers, so that the encapsulated packets can be transported securely over the internet.

Encryption protects data against unauthorized access from outside, ensuring that the data can only be read by authorized persons. Persons who do not have the encryption keys cannot make sense of the data even if they intercept the packets. VPN technologies generally use 128-bit encryption. However, higher encryption levels may require more processor power and may negatively affect system performance.

Authentication is a security mechanism that determines whether people trying to access the network are authorized. There are basically three different authentication methods. PPP (Point-to-Point Protocol) provides user authentication. IKE (Internet Key Exchange) performs authentication at the computer level. IPSec can authenticate with a computer certificate or pre-shared key.

8.4. VPN Protocols

8.4.1. PPTP (Point-to-Point Tunneling Protocol)

PPTP is a protocol that creates a tunnel between two points and transmits data over this tunnel (Vacca, J. R., 2024k). However, this protocol is not preferred today because it does not support encryption as a standard. Its details are defined in the RFC2637 document.

8.4.2. L2TP (Layer Two Tunneling Protocol)

L2TP is a tunneling protocol developed by Cisco and defined in the RFC2661 document. It provides tunneling at the Layer 2 level and works with IPSec for encryption to increase security (Vacca, J. R., 2024k).

8.4.3. IPSec (Internet Protocol Security)

IPSec is a widely used protocol that allows secure transportation through an encrypted tunnel and provides higher security levels by working in harmony with different security protocols. It has two operating modes: Transport and Tunnel. While only the data carried is encrypted in Transport mode, all data packets are encrypted in Tunnel mode (Vacca, J. R., 2024k).

8.4.4. SSTP (Secure Socket Tunneling Protocol)

SSTP provides secure tunneling and encryption using SSL/TLS protocols. These protocols, which are usually used for HTTPS traffic, can also be used for VPN connections and are known as SSL VPN. It provides additional security by using SSL certificates for authentication and is preferred due to its ease of configuration (Vacca, J. R., 2024k).

9. Network Monitoring and Update

Continuous monitoring of network security and the effectiveness of security policies is necessary. In this way, new threats and weaknesses can be quickly addressed and security policies and measures can be updated.

9.1. SIEM (Security Information and Event Management)

It is a security technology used to collect information security management on a central platform (González-Granadillo et al., 2021). SIEM is used to detect, monitor, manage and analyze and store security events in real time. SIEM is passive preventive systems that produce meaningful relationships between logs by performing operations according to defined rules on collected logs and warn and guide system administrators (Vacca, J. R., 2012). It has detailed logging and correlation features. Alerts are triggered and alert generation is provided thanks to correlations. For example, we can give a warning if a user tries to enter an incorrect password 5 times in 2 minutes on their corporate computer.

9.2. EDR (Endpoint Detection and Response)

EDR is a cybersecurity technology used to protect endpoint devices such as computers, servers, mobile devices, and to detect threats on endpoints and take action (Arfeen et.al, 2021). EDR systems continuously monitor and analyze activities on endpoints and provide rapid response to potential security threats (Kaur et.al, 2024).

It provides the opportunity to monitor and detect many deep attack methods that antivirus programs cannot detect. When an abnormal process is detected between network nodes (clients) or at any network end, the relevant end and network are automatically filtered. The network end that caused the alarm is marked and the reactions, path, source and movements on the network are monitored to try to determine the attack activity and source. EDR systems can offer defense tactics and suggestions as a result of detailed examination and analysis of the attacks they detect.

9.3. SOAR (Security Orchestration, Automation and Response)

It is a security technology designed for security operations centers (SOCs) (Laird, J. E., 2012). Its main purpose is to make the management of security incidents faster, more effective and automated. SOAR consists of three basic components.

Orchestration, integrates different security tools and systems and ensures that they work together (Islam et.al, 2020). For example, it combines data from different systems such as SIEM (Security Information and Event Management) and firewall.

Automation, Automates repetitive tasks (Islam et.al, 2020). For example, automatically quarantines an email after a phishing email is detected.

Response, provides fast and effective response to security incidents (Islam et.al, 2020). Reduces the need for human intervention with predefined workflows and playbooks.

10. Vulnerability Scanning and Penetration Tests

Effective methods used to test the functionality and adequacy of the measures taken are Vulnerability Scanning and Penetration Tests (Vacca, J. R.,2024i). These applications enable the detection of the effects of possible vulnerabilities and possible attack risks (Vegesna, V. V. (2022).

10.1. Vulnerability Scanning

The aim of the vulnerability scanning process is to find possible vulnerabilities by using automated tools or by checking with human eyes. Automatic vulnerability scanning tools check whether previously known security vulnerabilities are present in the network systems (Vacca, J. R.,2024i). For vulnerabilities that these tools cannot detect, checks must be made with human eyes. The findings obtained as a result of the Vulnerability Scanning are reported and used to eliminate the vulnerabilities.

10.2. Penetration Testing

It is the process of examining the security of information systems from the perspective of an attacker, within legal and ethical limits, based on a confidentiality agreement and a certain scope. Penetration tests include the vulnerability scanning step as a scope.

Possible weaknesses are detected with automated tools and/or human eyes. While vulnerability scanning focuses on detecting security vulnerabilities in the system, penetration testing allows the analysis of the weak points of the system by exploiting these vulnerabilities in an authorized manner (Vegesna 2022). The findings obtained during the penetration testing process are exploited with the techniques and methods used by the attackers and access is provided to the target systems(Vacca, J. R.,2024j).

Horizontal progress is attempted by accessing other systems in the network with the new information and findings obtained from the information systems that are entered. At the same time, vertical progress is attempted by trying to access higher authorized user accounts from low authorized user accounts.

The findings obtained are reported in detail and used to close the vulnerabilities.

11. Conclusion

Many technical measures that can be taken to ensure network security, such as network segmentation, firewalls, intrusion detection and prevention systems, will form a basic security layer. However, since security is not a phenomenon that can be provided only with technological solutions, technical measures alone cannot be expected to be sufficient. While technical measures provide powerful tools to detect and prevent threats, the effectiveness of the measures taken depends on correctly defined and implemented security policies.

Technical measures should be based on administrative measures such as security policies that emerge as a result of the analyses. In order to reduce the risks caused by non-technical elements such as human factors and organizational weaknesses, security policies, procedures, regulations and guides that will guide users should be defined and implemented realistically. Administrative measures increase the effectiveness of technical measures and prevent human-related errors.

Technical and administrative measures taken by conducting penetration tests and operating internal audit mechanisms should be constantly inspected, and policies and measures should be updated according to the findings obtained as a result of the controls.

Institutions' holistic approach to network security and effective implementation of technical and administrative measures together will enable the creation of a structure that is more resilient against cyber threats.

References

3. Fırlar, T. (2003). IP ağlarında güvenlik sorunlarının çözümüne yönelik bir mekanizma önerisi. *SAÜ Fen Bilimleri Enstitüsü Dergisi,* 7(1), 9-16. https://dergipark.org.tr/tr/download/article-file/193184

4. Tekerek, M. (2008). Bilgi güvenliği yönetimi. *KSÜ Fen ve Mühendislik Dergisi,* 11(1), 132-137. https://dergipark.org.tr/tr/download/article-file/423183

5. Can, Ö., & Akbaş, M. F. (2014). Kurumsal ağ ve sistem güvenliği politikalarının önemi ve bir durum çalışması. *TÜBAV Bilim Dergisi,* 7(2), 16-31. https://dergipark.org.tr/tr/pub/tubav/issue/21535/230996

6. Kumar, A., & Malhotra, S. (2015). Network security threats and protection models. Technical Report – CSE- 101507, Indian Institute of Technology Kanpur. https://arxiv.org/abs/1511.00568

7. Coulibaly, K. (2020). An overview of intrusion detection and prevention systems. Bradford University Faculty of Engineering and Informatics Technical Report. https://arxiv.org/abs/2004.08967

8. Liang, J., & Kim, Y. (2022). Evolution of firewalls: Toward securer network using next generation firewall. *12th Annual Computing and Communication Workshop and Conference (CCWC),* 752-759. https://doi.org/10.1109/CCWC54503.2022.9720435

9. Li, L., Lu, H., & Li, X. (2014). Assessment and application of network access control technologies. *2014 2nd International Conference on Systems and Informatics (ICSAI 2014),* 670-675. https://doi.org/10.1109/ICSAI.2014.7009264

10. Mehdizadeh, A., Suingg, K., Mohammadpoor, M., & Harun, H. (2017). Virtual local area network (VLAN): Segmentation and security. *Proceedings of the Third International Conference on Computing Technology and Information Management (ICCTIM2017),* 78-89. ISBN: 978-1-941968-45-1. https://www.academia.edu/35497133/Virtual_Local_Area_Network_VLAN_Segmentation_and_Security

11. Nourildean, S. W., Mohammed, Y. A., & Attallah, H. A. (2023). Virtual local area network performance improvement using ad hoc routing protocols in a wireless network. *Computers*, 12(28). https://doi.org/10.3390/computers12020028

12. Makeri, Y. M., Cirella, G. T., Galas, F. J., Jadah, H. M., & Adeniran, A. O. (2021). Network performance through virtual local area network (VLAN) implementation & enforcement on network security for enterprise. *International Journal of Advanced Networking and Applications*, 12(6), 4750-4762. https://doi.org/10.35444/IJANA.2021.12604

13. Alshalan, A., Pisharody, S., & Huang, D. (2016). A survey of mobile VPN technologies. *IEEE Communications Surveys & Tutorials*, 18(2), 1177-1199. https://doi.org/10.1109/COMST.2015.2496624

14. Solisch, T. (2022). Comparison of VPN technologies. Faculty of Engineering and Information Technology, OTH Regensburg Technical Report. Retrieved from https://arxiv.org/pdf/5468-vpn.pdf.

15. González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security Information and Event Management (SIEM): Analysis, trends, and usage in critical infrastructures. *Sensors,* 21(4759). https://doi.org/10.3390/s21144759

16. Arfeen, A., Ahmed, S., Khan, M. A., & Jafri, S. F. A. (2021). Endpoint detection & response: A malware identification solution. *Proceedings of the International Conference on Cyber Warfare and Security (ICCWS)*, 1-8. https://doi.org/10.1109/ICCWS53234.2021.9703010

17. Karantzas, G., & Patsakis, C. (2021). An empirical assessment of endpoint detection and response systems against advanced persistent threats attack vectors. *Journal of Cybersecurity and Privacy,* 1(3), 387–421. https://doi.org/10.3390/jcp1030021

18. Islam, C., Babar, M. A., & Nepal, S. (2020). A multi-vocal review of security orchestration. *Journal of Cybersecurity and Privacy*, 1(3), 387–421. https://doi.org/10.3390/jcp1030021

19. Vegesna, V. V. (2022). Utilising VAPT technologies (Vulnerability Assessment & Penetration Testing) as a method for actively preventing cyberattacks. International Journal of Management, *Technology and Engineering*, 12(7), 81-94. https://www.researchgate.net/publication/374949898.

20. ISO(International Organization for Standardization), (2022a). ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection - Information security management systems - Requirements (Annex A.5.1, Information Security Policies). Geneva, Switzerland: ISO.

21. ISO(International Organization for Standardization), (2022b). ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection - Information security management systems - Requirements (Clause 6.1, Planning Actions to Address Risks and Opportunities). Geneva, Switzerland: ISO.

22. ISO(International Organization for Standardization), (2022c). ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection - Information security management systems - Requirements (Annex A.5.15, Access Control). Geneva, Switzerland: ISO.

23. Astrida, D. N., Saputra, A. R., & Assaufi, A. I. (2016). Design a resilient network infrastructure security policy framework. *International Journal of Security and Its Applications*, 10(2), 247-258. https://indjst.org/articles/design-a- resilient-network-infrastructure-security-policy-framework

24. Marttin, V., & Pehlivan, İ. (2010). ISO 27001: 2005 Bilgi Güvenliği Yönetimi Standardı ve Türkiye'deki Bazı Kamu Kuruluşu Uygulamaları Üzerine Bir İnceleme. *Mühendislik Bilimleri ve Tasarım Dergisi*, 1(1), 49-56.

25. Marttin, V. (2014). Saldırı tespit sistemlerinde yapay sinir ağlarının kullanımı ve başarımlarının incelenmesi (Master's thesis, Bilecik Şeyh Edebali Üniversitesi, Fen Bilimleri Enstitüsü).

26. Marttin, V., & İmal, N. (2015). Yapay Sinir Ağları Kullanarak, Bilgisayar Ağlarında Saldırı Tespit Sistemi ve Başarımlarının İncelenmesi. *Gaziosmanpaşa Bilimsel Araştırma Dergisi*, (11), 21-40.

27. Mukkamala, P. P., & Rajendran, S. (2020). A Survey on the Different Firewall Technologies. International Journal of Engineering *Applied Sciences and Technology*, 5(1), 363-365. https://www.ijeast.com/papers/363- 365,Tesma501, IJEAST.pdf

28. Vacca, J. R. (Ed.).(2024a). Types of firewalls. Computer and Information Security Handbook 4th Edition (pp. 308).

29. Vacca, J. R. (Ed.).(2024b). Host and network firewalls. Computer and Information Security Handbook 4th Edition (pp. 1269). (Netgate,2024)

30. Cheswick, W. R., Bellovin, S. M., & Rubin, A. D. (2003). Firewalls and internet security: Repelling the wily hacker (2nd ed.). Addison-Wesley (pp. 176-178).

31. Zhang, Y., & Wang, X. (2021). Firewall filtering technology and application based on static packet filtering. *In Proceedings of the 2021 International Conference on Computer Engineering and Artificial Intelligence* (pp. 123-130). Springer.

32. Klein, A. (2021). Subverting Stateful Firewalls with Protocol States (Extended Version). arXiv. https://arxiv.org/abs/2112.09604

33. Netgate. (n.d.). Hardware sizing guidance. Retrieved November 22, 2024, from https://docs.netgate.com/pfsense/en/latest/hardware/size.html

34. Vacca, J. R. (Ed.).(2024). Application-layer firewalls: Proxy servers. Computer and Information Security Handbook 4th Edition (pp. 308).

35. Wessels, D. (2004). Chapter 9. Interception Caching. Squid: The definitive guide. O'Reilly Media. (pp. 183-185)

36. Vacca, J. R. (Ed.).(2024c). Intrusion Detection. Computer and Information Security Handbook 4th Edition (pp. 1310–1311).

37. Vacca, J. R. (Ed.).(2024c). Intrusion Prevention. Computer and Information Security Handbook 4th Edition (pp. 1310–1311).

38. ISO(International Organization for Standardization), (2022d). ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection - Information security management systems - Requirements (Annex A.8.22, Segregation of networks). Geneva, Switzerland: ISO.

39. Vacca, J. R. (Ed.).(2024d). Secure design through network access controls. Computer and Information Security Handbook 4th Edition (pp. 298).

40. Vacca, J. R. (Ed.).(2024e). Host access: partitioning. Computer and Information Security Handbook 4th Edition (pp. 1063).

41. IEEE(Institute of Electrical and Electronics Engineers), (2022). IEEE Standard for Local and Metropolitan Area Networks—Bridges and Bridged Networks (IEEE Std 802.1Q-2022). IEEE. https://doi.org/10.1109/IEEESTD.2022.10004498

42. Vacca, J. R. (Ed.).(2024f). Demilitarized Zones. Computer and Information Security Handbook 4th Edition (pp. 1270-1271).

43. Viecco, C. (2013a). Handling Wireless Guest Access. Wireless network security: A beginner's guide. McGraw-Hill Education.(pp 251-261)

44. TBMM(Türkiye Büyük Millet Meclisi), (2007). İnternet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele edilmesi hakkında kanun (5651 sayılı kanun). Resmî Gazete, Sayı: 26530. https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5651&MevzuatTur=1&MevzuatTertip=5

45. BTK(Bilgi Teknolojileri ve İletişim Kurumu),(2013). İnternet toplu kullanım sağlayıcıları hakkında yönetmelik. Resmî Gazete, Sayı: 30035. https://www.resmigazete.gov.tr/eskiler/2017/04/20170411-3.htm

46. Viecco, C. (2013b). Network Access Control. Wireless network security: A beginner's guide. McGraw-Hill Education.(pp 279)

47. Vacca, J. R. (Ed.).(2024g). Plugging the gaps: nac and access control. Computer and Information Security Handbook 4th Edition (pp. 148-149, 280-281).

48. Vacca, J. R. (Ed.).(2024h). Virtual Private Network Types. Computer and Information Security Handbook 4th Edition (pp. 1016–1017).

49. Vacca, J. R. (Ed.).(2012). Security Monitoring Mechanisms. Computer and Information Security Handbook (pp. 250).

50. Kaur, H., Sanjaiy, D. S. L., Paul, T., Thakur, R. K., Reddy, K. V. K., Mahato, J., & Naveen, K. (2024). Evolution of Endpoint Detection and Response (EDR) in Cyber Security: A Comprehensive Review. *E3S Web of Conferences*, 556, Article 01006. https://doi.org/10.1051/e3sconf/202455601006

51. Laird, J. E. (2012). Society for the Study of Artificial Intelligence and Simulation of Behaviour. *The Soar Cognitive Architecture*. AISB Quarterly, (134), 1–4. https://www.academia.edu/75134727/The_Soar_Cognitive_Architecture

52. Vacca, J. R. (Ed.).(2024i). What Is Vulnerability Assessment. Computer and Information Security Handbook 4th Edition (pp. 537-539).

53. Vacca, J. R. (Ed.).(2024j). Penetration Testing. Computer and Information Security Handbook 4th Edition (pp. 1283).

54. Cheswick, W. R., Bellovin, S. M., & Rubin, A. D. (2003). Application-Level Filtering. Firewalls and internet security: Repelling the wily hacker (2nd ed.). Addison-Wesley (pp. 185-186).

55. Tarlacı ,M. F., Çetin,G. & Tenruh, M (2019). Dinamik VLAN yapılandırmasının kablosuz yerleşke alan ağlarında incelenmesi. *Uluslararası Teknolojik Bilimler Dergisi*, 11(1), 45-52. https://dergipark.org.tr/tr/download/article-file/817104

56. Vacca, J. R. (Ed.).(2024k). Virtual Private Networks. Computer and Information Security Handbook 4th Edition (pp. 1020).