Gill, M. A., Ahmad, N., Khan, M., Asghar, F., and Rasool, A. (2023). Cyber Attacks Detection through Machine Learning In Banking. *Bulletin of Business and Economics,*12(2), 34-45. https://doi.org/10.5281/zenodo.8310116

Bulletin of Business and Economics
ISSN - 2409 - 9368

CYBER ATTACKS DETECTION THROUGH MACHINE LEARNING IN BANKING

MOHSIN ASAD GILL[1], NAVEED AHMAD[2], MADIHA KHAN[3], FAHAD ASGHAR[4], AWAIS RASOOL[5]

ABSTRACT

Cyberattacks may cause a wide range of problems, from power outages to broken military equipment to the loss of vital information like patient medical records. Due to the huge monetary worth of the information banks keep, they are a prime target for cybercriminals. The larger the digital footprints of banks, the easier it is for hackers to target them. This study examines the Banking Dataset for indicators of cyber attacks on financial institutions. In this research, CYBER attacks have been predicted using a combination of classification techniques. We have increased the complexity of generic model architecture in an effort to boost their performance. The support vector machine (SVM) was not the only technique we utilized; the k-nearest neighbors (KNN) and random forest (RF) methods were also used. When compared to the KNN and RF, the SVM's detection accuracy of 99.5% was much superior. When compared to KNN, RF, and other established ML/DL techniques, the SVM has been determined to be the most reliable.

KEYWORDS: machine learning, support vector machine, cyberattacks

1. INTRODUCTION

In the first half of 2021, ransomware assaults climbed 1318 percent, disproportionately affecting banks (Sahingoz et al. 2019). BEC assaults may have increased 4% due to COVID-19 (Kambourakis et al. 2017). Bank hacks are rising. Banks are linked, so a cyberattack on one might threaten another. State-sponsored cyberattacks threaten US banks (Ezekiel et al. 2017).

As internet and mobile banking usage rises, so does cybercrime. Cybercrime includes credit card fraud, spamming, ATM robberies, and identity theft (Javeed et al. 2021). Valuable banking data is vulnerable. Hackers can profit from financial and banking data in several ways. Bank digital footprints increase their attack surface (Kushwah & Ranga 2020). Cyberattacks may disrupt power, military equipment, and sensitive information. They can steal medical records. They can interrupt phone and computer networks, destroying data and systems (Osanaiye et al. 2016).

Data makes banking susceptible. Hackers can profit from financial and banking data in several ways. Machine learning solves informational issues. ML/DL models apply to biological (Ahmad et al. 2022, Ahmad et al. 2022, Ahmad et al. 2021, Ahmad et al. 2020) agricultural (Wang et al. 2022, Ahmad et al. 2020), and IoT datasets (Ali et al. 2020).

This study's key findings: Based on their high performance, SVM, KNN, and RF were recommended for cyber-attack categorization using Banking Dataset. Cyber threat detection with SVM, KNN, and RF has never been compared.

Training variables affected classification accuracy, precision, recall, F1-score, and time complexity (ms).

SVM, KNN, and RF were evaluated to identify the best ML model assessment model. SVM outperforms KNN/RF/ML/DL. This study has five parts. Section 1 introduces this investigation; Section 2 shows related research. Section 3 covers study methods, whereas Section 4 covers results. Section 5 ends.

2. LITERATURE REVIEW

New cyber threat Middlebox Investigated. Hosts are constantly monitored, filtered, and altered. Unlike routers and switches, middleboxes can do full packet DPI analysis. Historically, middleboxes have served as firewalls. In order to keep tabs on all incoming and outgoing data, censoring countries set up enormous filtering middleboxes either at their borders or inside their ISPs. Censoring firewalls scan unencrypted traffic, DNS queries, and TLS SNI fields for prohibited phrases and domains. Connections are disrupted by censoring intermediaries. Inject RST packets to close

[1] PhD Scholar, School of Business, Southern Queensland University, Australia, mag_gill@hotmail.com
[2] Department of Computer Science, Comsats University Islamabad, Pakistan, naveed.uom.cs@gmail.com
[3] MBA, NUST Business School, National University of Sciences and Technology, Islamabad, Pakistan, Madihakhan18@live.com
[4] Department of Business Administration, Thal University Bhakkar, Pakistan, fahadasghar214@gmail.com
[5] Department of computer science, University of Agriculture Faisalabad, Pakistan, awaisrasool7373@gamil.com

the connection and block pages for prohibited HTTP requests to prevent data from being sent. Different types of connections are blocked by middleboxes. Middleboxes do connection analysis over many packets to identify reordering or loss of packets. To some extent, middleboxes may lose bidirectional packets. Several paths are possible for data traveling between two hosts over the Internet. Only TCP traffic between clients and servers is visible to a middlebox. Middleboxes may now prevent connections without inspecting packets thanks to TCP reassembly. Due to its tolerance for lost packets, middleboxes may be tricked by reflection attackers into believing the three-way handshake is complete. It's possible that middlebox packets, and block pages in particular, are a good fit for reflected amplification. We demonstrate how middleboxes may be used to function as powerful amplifiers.

The effects of cybercrime on banks and how they might protect themselves from it are examined in Chayomchai et al. (Chayomchai et al. 2020). Targets include financial institutions. Information and money are stolen in Indian bank hacks. This report recommends that businesses create a unique cyber-security strategy to protect their most valuable data. Examining government websites, journals, and research projects as secondary sources of data, this article assesses cyber dangers and crimes that resulted in significant financial losses. The findings of this study will provide light on the cyber regime for the public and the financial sectors. Symmetrical LDA DoS attack predictions may be made with limited accuracy using unannotated tweets and Kullback-Leibler divergence. Module use is limited by light monitoring. Events on Twitter that aren't attacks are less likely to be misunderstood as Denial of Service attacks during the detection period. In a second classification layer, human-annotated tweets about denial-of-service attacks may weed out the noise. Industry-specific models are available to others via weakly-supervised learning .

The robust approach developed by Alimolaei et al. (Alimolaei et al. 2015) can detect untrustworthy web-based bank customers. Developers of the system used fuzzy theory to account for the ambiguity of user input. The R.O.C. curve accuracy of the fuzzy expert system was 94%. Online banking could benefit from this expert system. Referencing first. There are cyber threats associated with online banking (Fang et al. 2011, Diro et al. 2021). The application boundaries are protected by the cyberbanking security. Hardware and software are protected in many ways.

Online banking fraud detection was developed by Salem et al. (Salem et al. 2022). Score fraud in both real-time online and physical transactions. Huge transaction logs in Gbase may be analyzed using tools like Kafka, Spark, and MPP. They put their strategy to the test on a large database of online banking transactions. These holes should be filled by the author's research. Cybercrime datasets are examined and problems are identified using K-Means, Influenced Association Classifier, and J48 Prediction Tree (Fang et al. 202, Gupta et al. 2021). K-Means clusters related to external factors. Cybercrime predictions are made using K-means classifiers with J48 centroids. Bank cybercrime may be predicted using K-Means, Influenced Association Classifier, or J48 Prediction Tree. Cybersecurity efforts should be funded by the author's government.

Current issues with banks and credit card companies were explored in (Diro et al. 2021, Saeedi 2019). To find a solution, you must first understand the issue. Knowledge about cyber threats helps banks avoid harm. Restrict access based on user IP and browsing session (Kamruzzaman 2021, Jegadeesan et al. 2020). Web pages are often requested more faster by automated attack sources than by human users. Security for apps and networks is essential. Spoofing, corrupted packets, and incomplete TCP handshakes are all used in cyberattacks. Application layer attacks drain resources from computers. Infection may be avoided with the use of monitoring for unusual user activity and application attack signatures. Traces of cyberattacks may be found. In many cyberattacks, hackers will utilize malicious HTTP requests. HTTP headers are repeated by Loris the Slow. In the digital realm, visitors may see blank pages. Websites may experience downtime due to attacks.

Mahmood and colleagues use HMMs to identify and stop fraudulent transactions in online banking (Mehmood et al. 2021). The bank sends a one-time password to the customer's mobile device, which allows the bank to verify only legitimate transactions. To avert these kinds of catastrophic losses, financial institutions are increasingly turning to fraud detection and prevention technologies. Innovative fraud detection and prevention technology are helping banks throughout the world cut down on fraudulent Internet banking transactions. There is no way to tell whether an account is authentic or not. To better depict Indian financial institution hacks, we'll use a Hidden Markov Model and then fix it. Spoofing, brute-force attacks, buffer overflows, and cross-site scripting are all linked to Indian public and private banks (Ramapatruni et al. 2019, Hameed et al. 2022). Intruder detection and system monitoring are linked to issues including online identity theft, hacking, dangerous coding, DoS attacks, and credit card/ATM fraud (Hameed et al. 2022, Kaushik & Sharma 2010, Dilraj et al. 2019).

Blockchain technology improves online safety. The immutability, verifiability, anonymity, and lack of need for a trusted third party are just some of the ways in which blockchain technology has the potential to mitigate this devastating cyber threat. Blockchain-based cyber defense in many industries does not need references. The scope of this investigation is broad. New technologies for cyber defense need to be investigated, therefore R&D efforts should be consolidated.

Collaboration in detecting breaches across networks is aided by time zone detection. Each network's detection and false positive rates are weighted by time zone to determine the result of an attack. (Tahir Ullah 2019) Data weighting for detecting cyber attacks is proposed. Good detection was achieved with a 35% reduction in false positives using the suggested strategy. Our research describes these features (Javeed et al. 2020, Javeed et al. 2022), however, the best preventive measure has yet to be identified and implemented. In this research, we identify and characterize the best practices for designing defenses against denial-of-service and cyberattacks that use the HTTP protocol. Entropy and divergence measures from information theory are used by researchers for this purpose (Jegadeesan et al. 2020). Unique hacks may be detected using a novel LeCam divergence measure based on similarities in network traffic flow. The procedures are put to the test on datasets such as MIT's Lincoln and CAIDA. LeCam Divergence is superior than Kullbeck-Leibler, Bhattacharya, and Pearson.

A Deep Neural Network (DNN) for classification and a well-posed sparse Auto Encoder (AE) for feature learning can differentiate between harmful and safe cyber communications (Shaikh 2019). Adjust DNN and AE sensitivity to find assaults. Reducing overfitting (Huang 2020) requires minimizing reconstruction error, avoiding gradient inflation or disappearance, and building a compact network with fewer nodes. Ten best-in-class methods were used to evaluate the suggested solution. Results were thoroughly tested using the CICIDS2017 and NSL-KDD benchmark datasets. The suggested approach is superior.

For decades, cyberattacks have rendered networks useless. SDN makes possible novel cyber defenses. (Razib 2022) Describes two methods for detecting cyber attacks. A cyberattack's intensity may be gauged in part by its origin. K-Nearest Neighbors (KNN) was developed by ML experts specifically for such purpose. The author's methods outperform competing methods in spotting cyberattacks on real-world datasets. Insider assaults are more common among authorized users (Javeed et al. 2022). To counteract cyberattacks, EDIP is used. By transmitting information to an attack proxy, EDIP may identify malicious users. There is less disruption to the user base because of attacks now. Working less is possible with proxy load balancing. Researchers developed spectral gene set filtering (SGSF) to pre-filter large gene set collections in order to alleviate statistical power issues (Javeed et al. 2021, Javeed et al. 2022, Shaikh et al. 2019, Huang et al. 2020).

IDS ban lists. Intruders won't spend their time with such inefficient methods. Setup and automation of IDS may be performed using machine learning and deep learning (Huang et al. 2020). Model accuracy is affected by the quality of the training data. Datasets are used extensively in IDS. Rare database research on cyberattacks. There is research on cheap IoT hacks by Huang et al. (Huang et al. 2020). Introduce new cyberattacks. This layout is ideal for low-budget cyber attackers because of its detectability, durability, and low management costs. The effects of cyber-attacks using this architecture may be anticipated with the help of the novel botnet development model (Razib et al. 2022). Finally, we looked at the range of variability for three rival Cyber defense systems. Cyberattacks against the Internet of Things are explained in this study.

3. MATERIALS AND METHODS

Here are details on the data collection, methodology, and measurements. Figure 1 shows research using data from an open-source site that tracks cyberattacks (accessed on 2 February 2021). Open-source datasets.

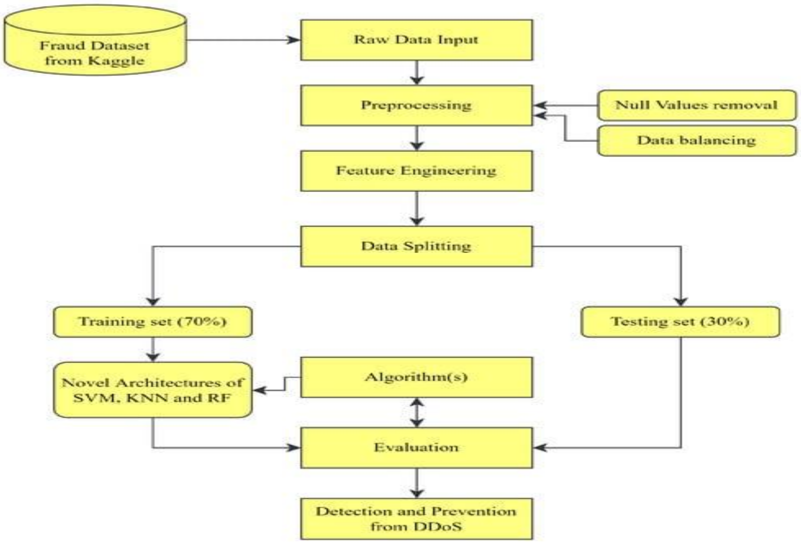


Figure 1. The proposed ML models' workflow in the context of the Bank dataset

Standard procedures preprocessed the data collection. Balancing procedures scaled and weighted data after missing values were removed. After feature extraction, we created a training set (70%) and a test set (30%). The training and testing sets train and test ML models.

3.1. DATASET DESCRIPTION

3.1.1. FRAUD-DETECTION DATASET

Banking Dataset tracks network intrusions. This nasty virus contains DoS. Table 1 and Figure 2 provide dataset properties.

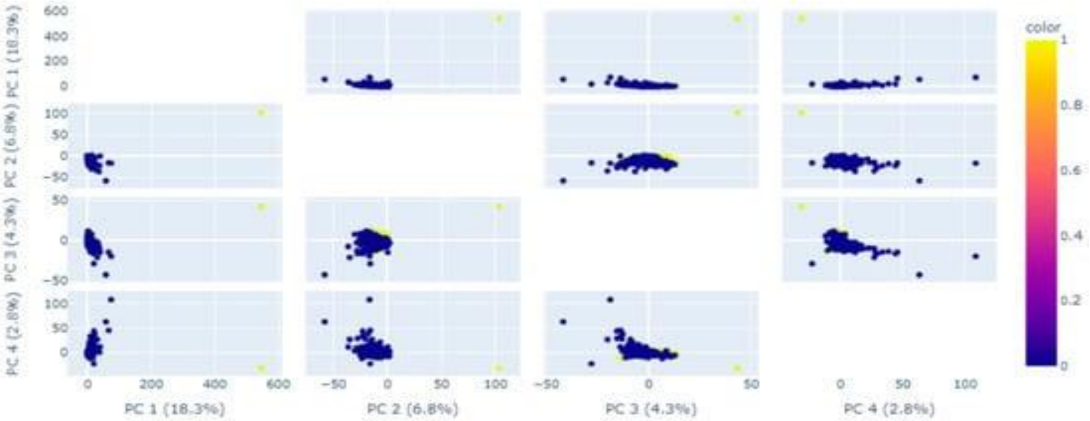


Figure 2. The redistribution of support

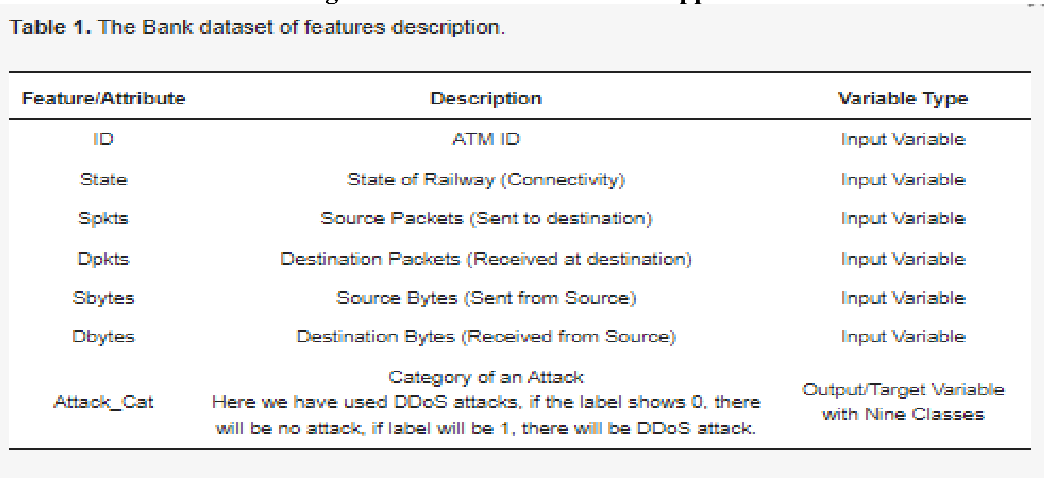


Table 1. The Bank dataset of features description.

Feature/Attribute	Description	Variable Type
ID	ATM ID	Input Variable
State	State of Railway (Connectivity)	Input Variable
Spkts	Source Packets (Sent to destination)	Input Variable
Dpkts	Destination Packets (Received at destination)	Input Variable
Sbytes	Source Bytes (Sent from Source)	Input Variable
Dbytes	Destination Bytes (Received from Source)	Input Variable
Attack_Cat	Category of an Attack Here we have used DDoS attacks, if the label shows 0, there will be no attack, if label will be 1, there will be DDoS attack.	Output/Target Variable with Nine Classes

Table 1. The Bank dataset of features description

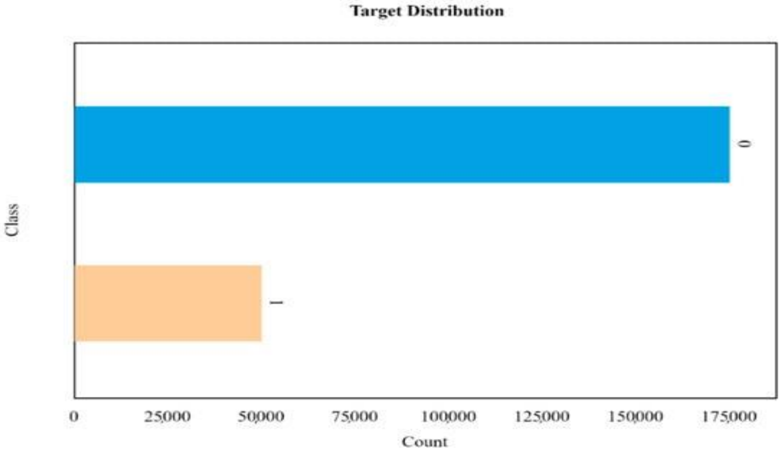


Figure 3: Bank dataset target distribution

Figure 2 shows 4 bank PC rearrangements. The heat map shows that a significant cyberattack is more likely when a PC's redistribution value exceeds 0.5. PC values below 0.5 reduce attack risk. Figure 3 shows the target class percentages. 50,000 cyberattacks are recorded.

These datasets assess the suggested approach. Preprocessed datasets help deep learning. An unsupervised homogeneity measure (k-means clustering) selects important properties from both datasets. The efficiency of deep learning models may be enhanced by using five-fold cross-validation. Attacks were categorized by three different machine learning algorithms. The data set is split into training (70%) and test (30%) sets. In empirical studies, testing 20-30% and teaching 70-80% yields the best results. Erasing source and destination IP addresses eliminates bias in identification. It may reject hosts with identical packet information by examining packet attributes instead Prioritizing Features

Figure 4 shows the feature correlation matrix. We designated the feature count columns col_0 through col_111 because there are so many characters and strings. Using k-means clustering, we ranked characteristics by relevance.

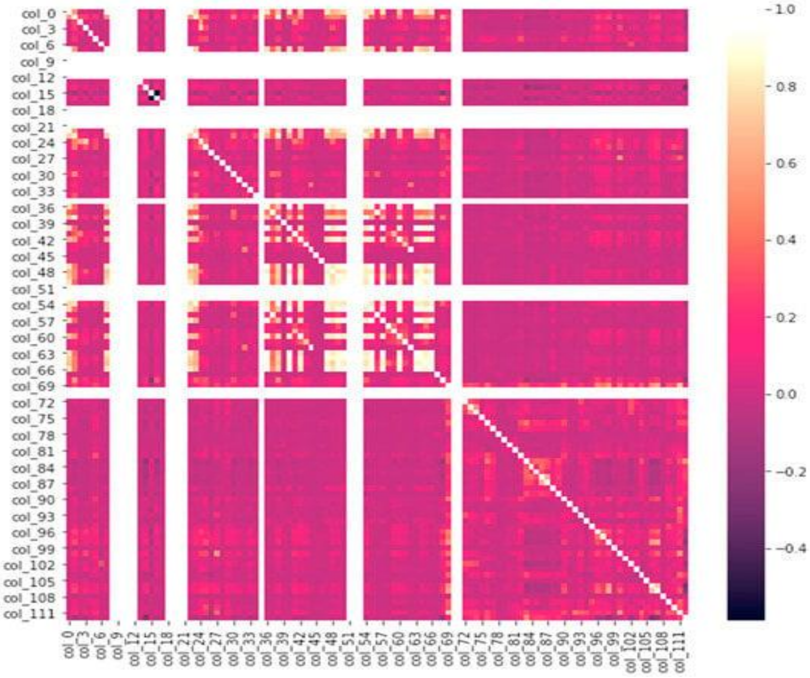


Figure 4. Presents feature correlation matrix

3.2. MACHINE-DATA-TRAINED MODELS

Supervised learning categorizes data based on previous learning. Based on an existing dataset, classification assigns new data to one of many established groups. KNN, SVM, and Random Forests identified banking sector cyberattacks.

3.2.1. THE SVM

SVMs excel in classification, regression, and outlier detection. SVMs are advantageous. It operates in high-dimensional surroundings.

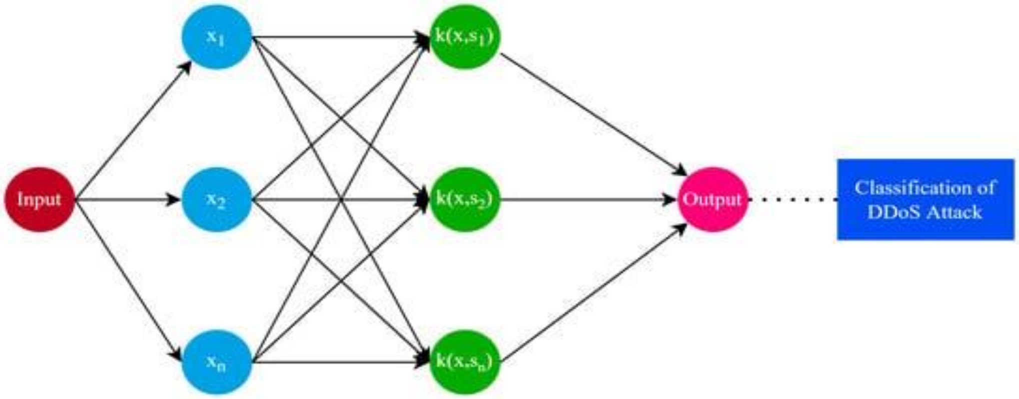


Figure 5. Basic architecture of SVM model for classification of Cyber-attacks

A unique SVM Classifier configuration classifies cyberattacks in this study. See Figure 5. Vector input layer (x). Compare the hidden layer's support vector (s, y) to the input layer's signal vector (x). Output neurons add hidden layer linear outputs O. To classify cyberattacks, we use the features of the SVM technique, switch data to extract characteristic values for training, the optimal classification hyperplane between normal data and cyberattack data, and test our model on test data.

3.2.2. RANDOM FORESTS

Classification and regression tasks can benefit from the use of random forests or random decision forests because they are an ensemble learning method that builds many decision trees at once. However, the accuracy of random forests is lower than that of gradient-boosted trees despite the fact that they outperform the former. In this study, random forests have been used for CYBER attack detection. In this study, we are classifying attacks by using the architecture of an RF Classifier. Its general architecture is shown in Figure 6. This model has been developed by assembling the logistic regression model into RF Classifier to improve both models' accuracy.

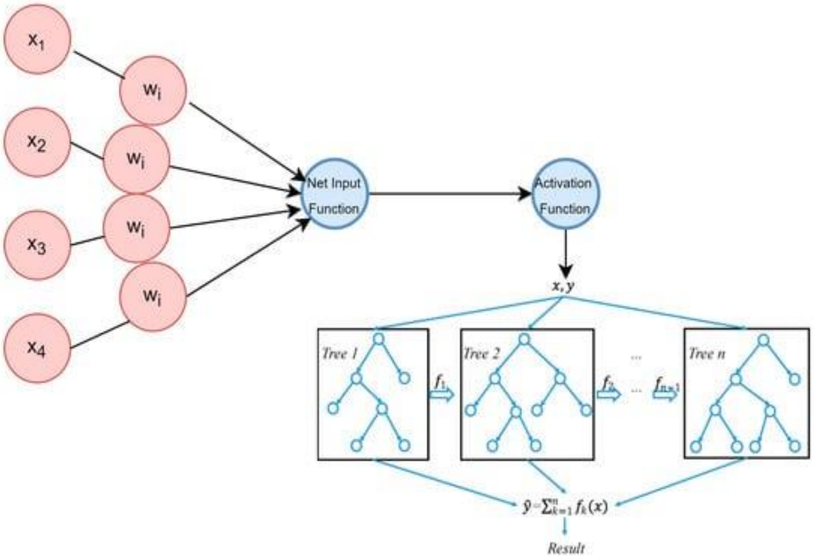


Figure 6. Cyber-attack categorization based on the RF model's framework

3.2.3. K-NEAREST NEIGHBORS

The abbreviation for "K-Nearest Neighbor" is "KNN." A.I. under human guidance. Use this strategy for classification and regression. To make a prediction or put anything into a category, look for its "K" closest neighbors. In this research, a novel KNN Classifier framework was used to label violent crimes. The components are shown in Figure 7. x is the input vector signal. The n nearest neighbors (y) of the hidden layer and the k-vector of the input signal determine the outcome. The linear sum, O, of the buried layer is the output of the neurons. KNN has excellent detection and little false positives [8]. KNN can detect online intrusions [9].

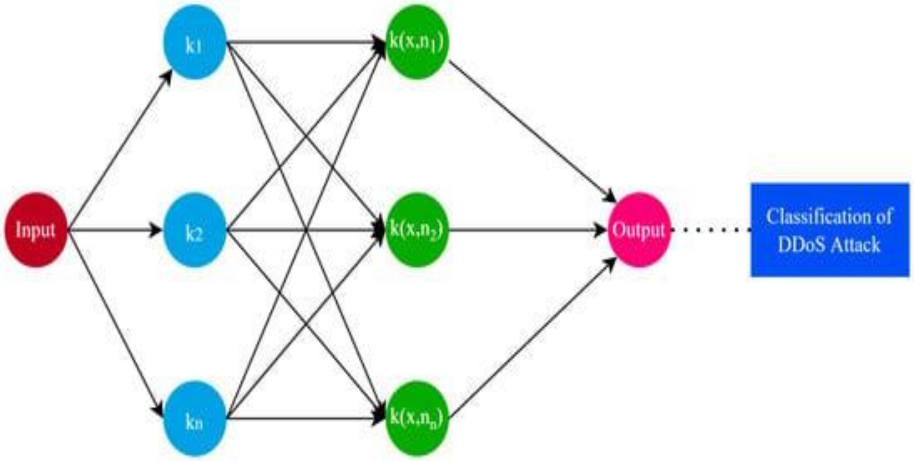


Figure 7. The Block diagram of KNN model for classification of Cyber-attacks

3.2.4. PERFORMANCE MEASURES

Accuracy, precision, recall, and F1 score measure algorithm performance. Confusion Matrix shows true and false positive rates. Strategies were evaluated using accuracy, precision, recall, and F1 Score. A confusion matrix shows categorized and misclassified clauses. Table 2 shows this study's metrics calculations.

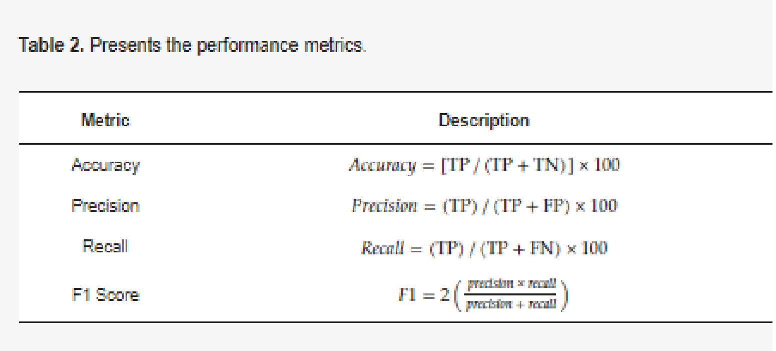


Table 2. Presents the performance metrics.

Metric	Description
Accuracy	$Accuracy = [\mathrm{TP} / (\mathrm{TP} + \mathrm{TN})] \times 100$
Precision	$Precision = (\mathrm{TP}) / (\mathrm{TP} + \mathrm{FP}) \times 100$
Recall	$Recall = (\mathrm{TP}) / (\mathrm{TP} + \mathrm{FN}) \times 100$
F1 Score	$F1 = 2\left(\frac{precision \times recall}{precision + recall}\right)$

Table 2. Performance Metrics

4. RESULTS

This section compares model results on sample data. SVM, RF, and KNN models were compared using various datasets. We'll test our model's categorization skills using the Fraud Dataset's nine assault incidents.

4.1. SVM MODEL EFFICIENCY

Support vector machines (SVMs) tackle two-classification problems using classification algorithms. SVM models can identify unknown text after training on category data. Figures 8 and 9 show the SVM model's effectiveness. SVM accuracy exceeds 99.8%:

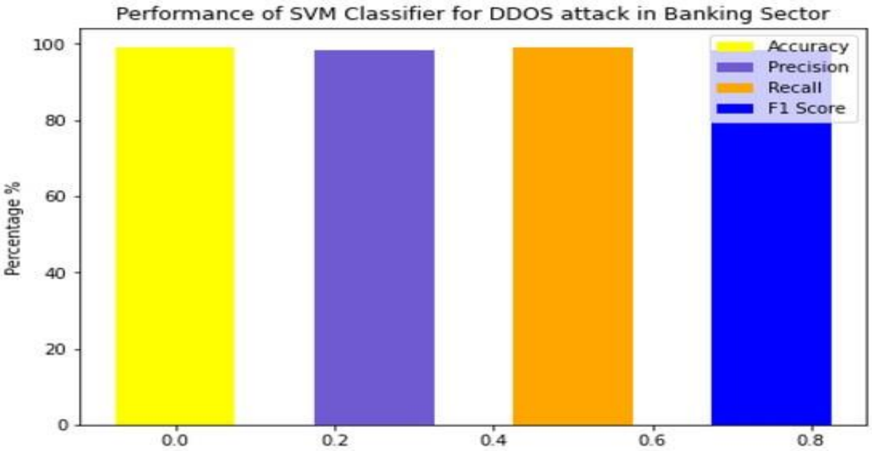


Figure 8. Metrics for measuring the effectiveness of the SVM model

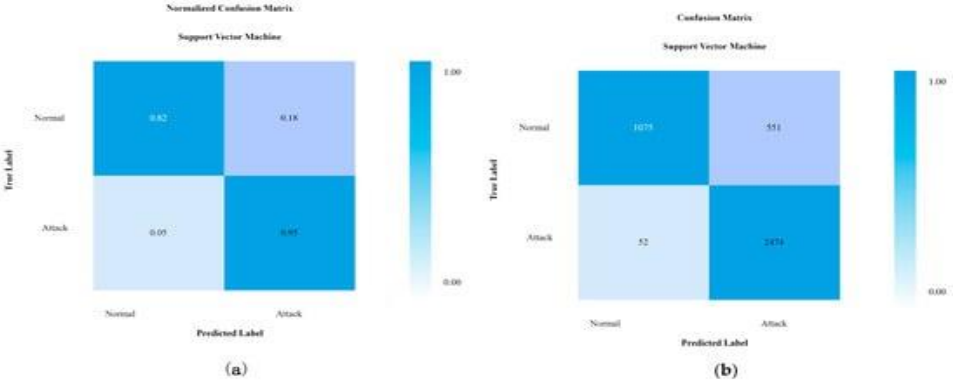


Figure 9. The SVM model's Confusion Matrix, (a) Normalized and (b), Un-normalized

4.2. RANDOM FORESTS' EFFICIENCY

"Random forest" categorization involves several decision trees. It uses bagging and feature randomization to create a forest of trees for each tree that predicts better than any single tree. Figures 10 and 11 exhibit RF model effectiveness. RF's accuracy is 97.5%.

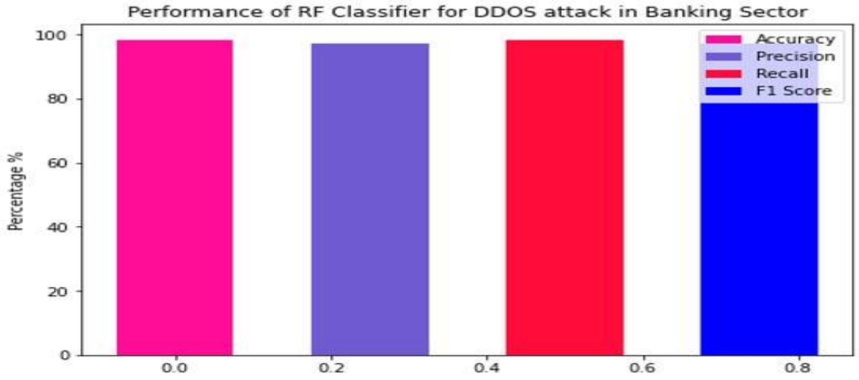


Figure 10. The performance evaluation metrics of RF model

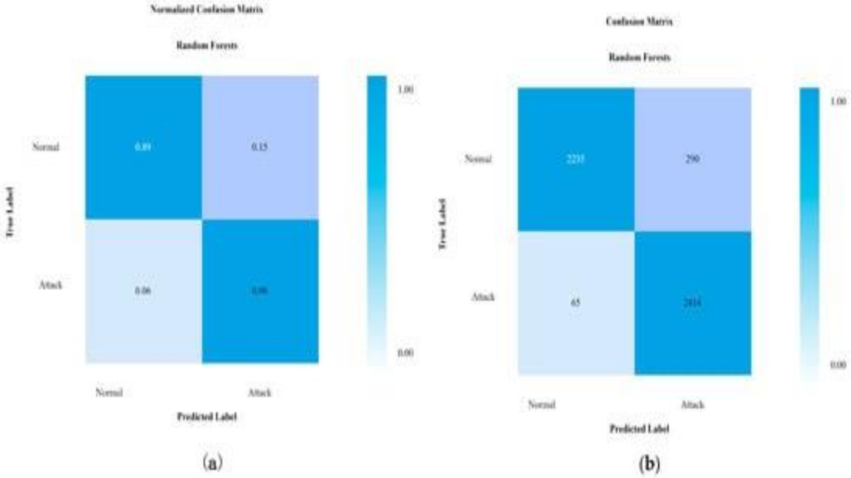


Figure 11. Confusion matrix of RF (a) Normalized (b) non-Normalized

4.3. THE EFFECTIVENESS OF KNNS

KNN may both classify and regress. Supervised machine learning algorithm that is simple to implement. Although simple to construct and understand, its significant negative is that its speed decreases with the amount of data. The effectiveness of the KNN model is seen in Figures 12 and 13. Accuracy of the KNN is 98.74%:

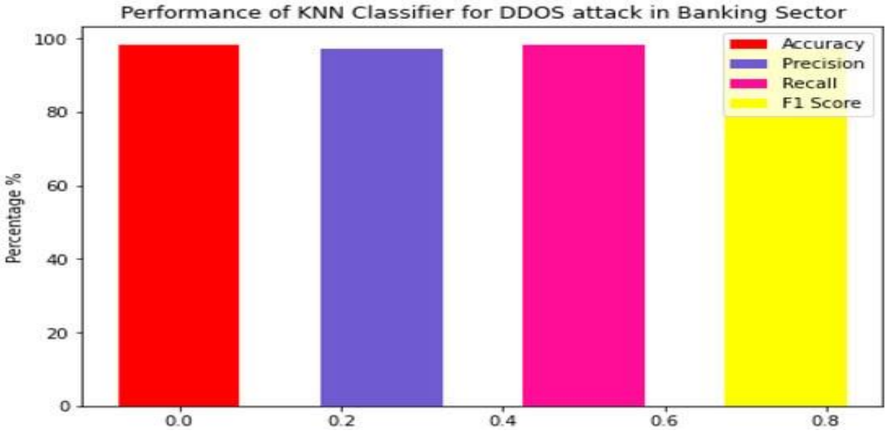
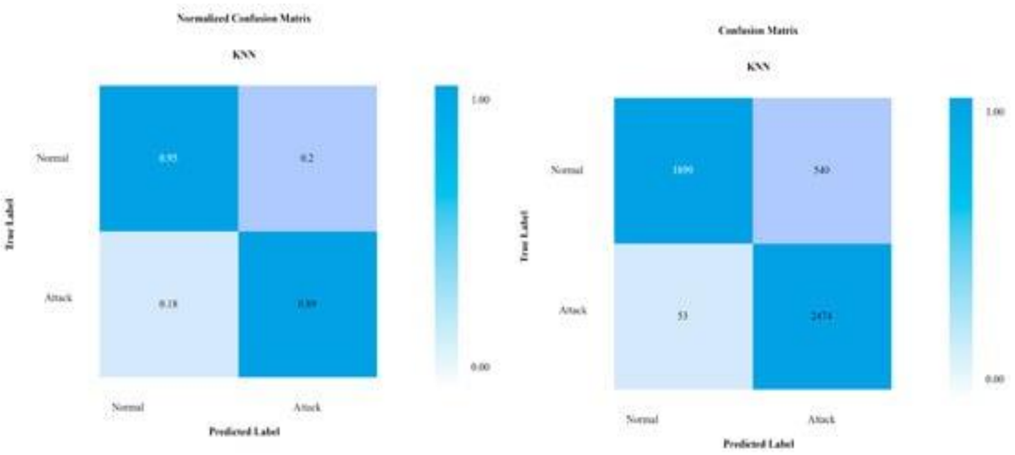


Figure 12. The KNN model's performance evaluation measures



(a)

(b)

Figure 13. The Confusion matrix of KNN (a) Normalized (b) Non-normalized

4.4. TIME COMPLEXITY (SEC)

The time complexity of the models (SVM, KNN, and RF) is crucial for evaluating their effectiveness. The time complexity (sec) of the models was shown in Figure 14. SVMs are more effective than KNN and RF models.

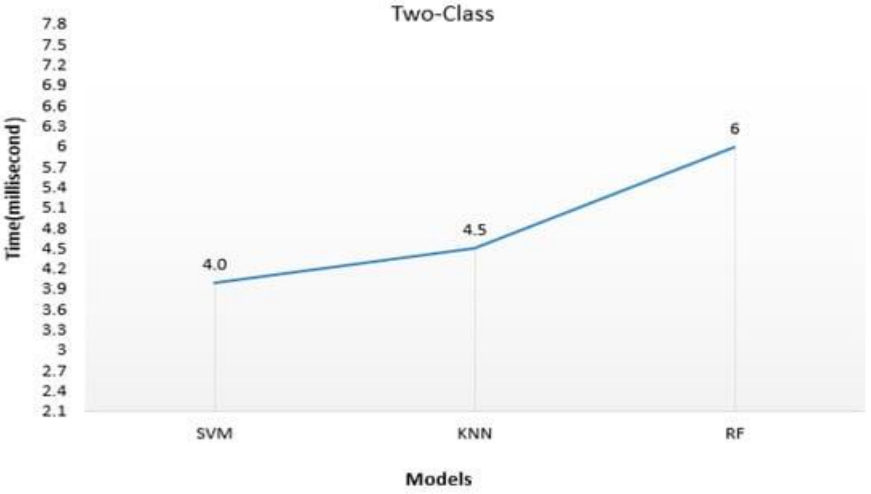


Figure 14. Presents the time complexity (sec) of the SVM, KNN, and RF model

Table 3. shows the comparative analysis of all models in the current study

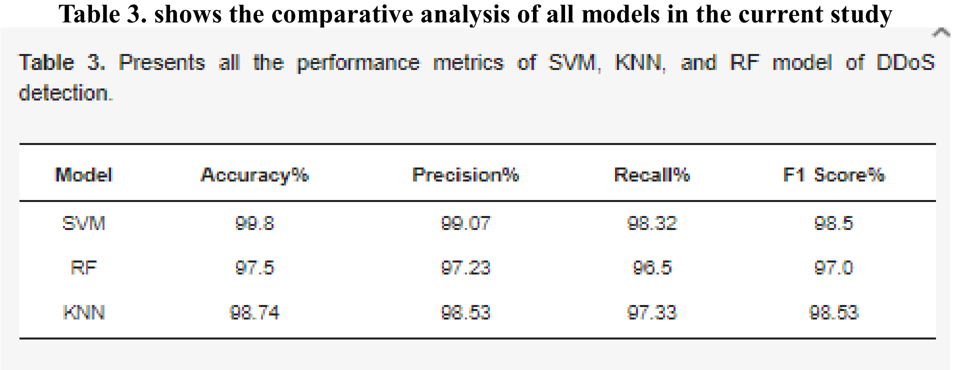


Table 3. Presents all the performance metrics of SVM, KNN, and RF model of DDoS detection.

Model	Accuracy%	Precision%	Recall%	F1 Score%
SVM	99.8	99.07	98.32	98.5
RF	97.5	97.23	96.5	97.0
KNN	98.74	98.53	97.33	98.53

Table 3. Presents all the performance metrics of SVM, KNN, and RF models of Cyber detection

Our suggested approach is shown to be more precise and effective than that of prior research. Table 4 below compares the present research to the state-of-the-art approaches (ML/DL) used in earlier studies.

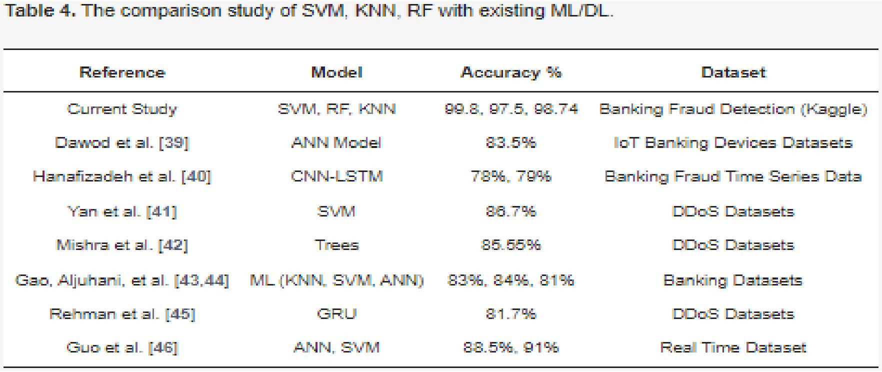


Table 4. The comparison study of SVM, KNN, RF with existing ML/DL.

Reference	Model	Accuracy %	Dataset
Current Study	SVM, RF, KNN	99.8, 97.5, 98.74	Banking Fraud Detection (Kaggle)
Dawod et al. [39]	ANN Model	83.5%	IoT Banking Devices Datasets
Hanafizadeh et al. [40]	CNN-LSTM	78%, 79%	Banking Fraud Time Series Data
Yan et al. [41]	SVM	86.7%	DDoS Datasets
Mishra et al. [42]	Trees	85.55%	DDoS Datasets
Gao, Aljuhani, et al. [43,44]	ML (KNN, SVM, ANN)	83%, 84%, 81%	Banking Datasets
Rehman et al. [45]	GRU	81.7%	DDoS Datasets
Guo et al. [46]	ANN, SVM	88.5%, 91%	Real Time Dataset

Table 4. The comparison study of SVM, KNN, and RF with existing ML/DL.

There are flaws in the suggested models as well. In order to complete the training process, the models needed a lot of processing power and specialized hardware, such as a powerful graphics processing unit (GPU).

5. CONCLUSIONS

Due to the high value of their data, financial institutions are susceptible to cyberattacks. Online banking credentials might be a lucrative target for hackers looking to cash in. Attackers may take advantage of banks' expanding digital footprints. We find cyberattacks on banks and other institutions using the Banking Dataset. Machine learning algorithms can spot potential problems in the banking system. We used RF, KNN, and SVM in our study. Accuracy ranged from 99.5% to 98.74% among three algorithms used to identify cyberattacks. When compared to other prominent machine learning/deep learning algorithms, such as KNN and RF, SVM showed superior performance stability. Since this approach can only be applied to historical data, we need real-time fraud detection solutions that employ supervised learning techniques.

References

Ahmad, I.; Liu, Y.; Javeed, D.; Ahmad, S. (2020). A decision-making technique for solving order allocation problem using a genetic algorithm. *IOP Conf. Ser. Mater. Sci. Eng. 853*, 012054.

Ahmad, I.; Liu, Y.; Javeed, D.; Shamshad, N.; Sarwr, D.; Ahmad, S. (2020). A review of artificial intelligence techniques for selection & evaluation. *IOP Conf. Ser. Mater. Sci. Eng, 853*, 012055.

Ahmad, I.; Ullah, I.; Khan, W.U.; Ur Rehman, A.; Adrees, M.S.; Saleem, M.Q.; Shafiq, M. (2021). Efficient algorithms for E-healthcare to solve multiobject fuse detection problem. *J. Healthc. Eng.* 9500304.

Ahmad, I.; Wang, X.; Zhu, M.; Wang, C.; Pi, Y.; Khan, J.A.; Li, G. (2022) EEG-Based Epileptic Seizure Detection via Machine/Deep Learning Approaches: A Systematic Review. *Comput. Intell. Neurosci.*, 6486570.

Ahmad, S.; Ullah, T.; Ahmad, I.; AL-Sharabi, A.; Ullah, K.; Khan, R.A.; Ali, M. (2022) A Novel Hybrid Deep Learning Model for Metastatic Cancer Detection. *Comput. Intell. Neurosci*, 8141530.

Ali, S.; Javaid, N.; Javeed, D.; Ahmad, I.; Ali, A.; Badamasi, U.M. (2020). A blockchain-based secure data storage and trading model for wireless sensor networks. In Proceedings of the International Conference on Advanced Information Networking and Applications, Caserta, Italy.

Alimolaei, S. (2015). An intelligent system for user behavior detection in Internet Banking. In Proceedings of the 2015 4th Iranian Joint Congress on Fuzzy and Intelligent Systems (CFIS), Zahedan, Iran.

Aljuhani, A. (2021). Machine learning approaches for combating distributed denial of service attacks in modern networking environments. *IEEE Access*, *9*, 42236–42264.

Aski, V.; Dhaka, V.S.; Kumar, S.; Parashar, A.; Ladagi, A. (2020). A multi-factor access control and ownership transfer framework for future generation healthcare systems. In Proceedings of the 2020 Sixth International Conference on Parallel, Distributed and Grid Computing (PDGC), Waknaghat, India, pp. 93–98.

Chayomchai, A.; Phonsiri, W.; Junjit, A.; Boongapim, R.; Suwannapusit, U. (2020). Factors affecting acceptance and use of online technology in Thai people during COVID-19 quarantine time. *Manag. Sci. Lett*, *10*, 3009–3016.

Dawod, A.; Georgakopoulos, D.; Jayaraman, P.P.; Nirmalathas, A.; Parampalli, U. (2022) IoT Device Integration and Payment via an Autonomic Blockchain-Based Service for IoT Device Sharing. *22*, 1344.

Dilraj, M.; Nimmy, K.; Sankaran, S. (2019). Towards Behavioral Profiling Based Anomaly Detection for Smart Homes. In Proceedings of the TENCON 2019–2019 IEEE Region 10 Conference (TENCON), Kochi, India, 17–20; pp. 1258–1263.

Diro, A., Chilamkurti, N., Nguyen, V. D., & Heyne, W. (2021). A comprehensive study of anomaly detection schemes in IoT networks using machine learning algorithms. *Sensors*, *21*(24), 8320.

Ezekiel, S.; Divakaran, D.M.; Gurusamy, M. Dynamic attack mitigation using SDN. In Proceedings of the 2017 27th International Telecommunication Networks and Applications Conference (ITNAC), Melbourne, VIC, Australia, 22–24 November 2017; pp. 1–6.

Fang, L.; Li, Y.; Liu, Z.; Yin, C.; Li, M.; Cao, Z.J. (2021). A Practical Model Based on Anomaly Detection for Protecting Medical IoT Control Services against External Attacks. *IEEE Trans. Ind. Inform*, *17*, 4260–4269.

Guo, C.; Wang, H.; Dai, H.N.; Cheng, S.; Wang, T. (2018). Fraud risk monitoring system for e-banking transactions. In Proceedings of the 2018 IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing, 16th Intl Conf on Pervasive Intelligence and Computing, 4th Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech), Athens, Greece, pp. 106–113.

Gupta, D.; Gupta, M.; Bhatt, S.; Tosun, A.S. (2021). Detecting Anomalous User Behavior in Remote Patient Monitoring. In Proceedings of the 2021 IEEE 22nd International Conference on Information Reuse and Integration for Data Science (IRI), Las Vegas, NV, pp. 33–40.

Hameed, M.; Yang, F.; Ghafoor, M.I.; Jaskani, F.H.; Islam, U.; Fayaz, M.; Mehmood, G.(2022). IOTA-Based Mobile Crowd Sensing: Detection of Fake Sensing Using Logit-Boosted Machine Learning Algorithms. *Wirel. Commun. Mob. Comput.* 6274114.

Hanafizadeh, P.; Amin, M.G. (2022). *The Transformative Potential of Banking Service Domains with the Emergence of FinTechs*; Palgrave Macmillan: London, UK, No. 0123456789.

Huang, K.; Yang, L.X.; Yang, X.; Xiang, Y.; Tang, Y.Y. (2020). A Low-Cost Distributed Denial-of-Service Attack Architecture. *IEEE Access*, *8*, 42111–42119.

Javeed, D., Gao, T., & Khan, M. T. (2021). SDN-enabled hybrid DL-driven framework for the detection of emerging cyber threats in IoT. *Electronics*, *10*(8), 918.

Javeed, D.; Gao, T.; Khan, M.T. (2022). Shoukat, D. A hybrid intelligent framework to combat sophisticated threats in secure industries. *22*, 1582.

Javeed, D.; Gao, T.; Khan, M.T.; Ahmad, I. (2021). A Hybrid Deep Learning-Driven SDN Enabled Mechanism for Secure Communication in Internet of Things (IoT). *21*, 4884.

Javeed, D.; Khan, M.T.; Ahmad, I.; Iqbal, T.; Badamasi, U.M.; Ndubuisi, C.O. (2020). Umar, A. An efficient approach of threat hunting using memory forensics. *Int. J. Comput. Netw. Commun. 8*, 37–45.

Jegadeesan, S.; Azees, M.; Ramesh Babu, N.; Subramaniam, U.; Almakhles, J.D. (2020). EPAW: Efficient Privacy Preserving Anonymous Mutual Authentication Scheme for Wireless Body Area Networks (WBANs). *IEEE 8*, 48576–48586.

Kambourakis, G.; Moschos, T.; Geneiatakis, D.; Gritzalis, S. Detecting DNS amplification attacks. In *CRITIS 2007: Critical Information Infrastructures Security*; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2008; Volume 5141 LNCS, pp. 185–196.

Kamruzzaman, M.M. (2021). New Opportunities, Challenges, and Applications of Edge-AI for Connected Healthcare in Smart Cities. In Proceedings of the 2021 IEEE Globecom Workshops (GC Wkshps), Madrid, Spain.

Kaushik, I.; Sharma, N. (2020). Black hole attack and its security measure in wireless sensors networks. In *Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario's*; Springer: Cham, Switzerland, Volume 1132.

Kushwah, G. S., & Ranga, V. (2020). Voting extreme learning machine based distributed denial of service attack detection in cloud computing. *Journal of Information Security and Applications*, *53*, 102532.

Lange, T.; Kettani, H. (2019). On Security Threats of Botnets to Cyber Systems. In Proceedings of the 2019 6th International Conference on Signal Processing and Integrated Networks (SPIN), Noida, India, pp. 176–183.

Mehmood, M.; Javed, T.; Nebhen, J.; Abbas, S.; Abid, R.; Bojja, G.R.; Rizwan, M. (2021). A hybrid approach for network intrusion detection. *Comput. Mater. Contin.*, *70*, 91–107.

Mhamane, S.S. (2012). Lobo, L.M.R.J. Internet banking fraud detection using HMM. In Proceedings of the 2012 Third International Conference on Computing, Communication and Networking Technologies (ICCCNT'12), Coimbatore, India.

Mishra, P.; Guru Sant, T. (2021). Role of Artificial Intelligence and Internet of Things in Promoting Banking and Financial Services during COVID-19: Pre and Post Effect. In Proceedings of the 2021 5th International Conference on Information Systems and Computer Networks (ISCON), Mathura, India, 22–23.

Oppliger, R.; Rytz, R.; Holderegger, T. (2009). Internet banking: Client-side attacks and protection mechanisms. *Computer*, *42*, 27–33.

Osanaiye, O., Choo, K. K. R., & Dlodlo, M. (2016). Analysing feature selection and classification techniques for DDoS detection in cloud. *Proceedings of Southern Africa Telecommunication*, 198-203.

Ramapatruni, S.; Narayanan, S.N.; Mittal, S.; Joshi, A.; Joshi, K. (2019). Anomaly Detection Models for Smart Home Security. In Proceedings of the 2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS), Washington, DC, USA, 27–29, pp. 19–24.

Razib, A.M.; Javeed, D.; Khan, M.T.; Alkanhel, R.; Muthanna, M.S.A. (2022). Cyber Threats Detection in Smart Environments Using SDN-Enabled DNN-LSTM Hybrid Framework. *IEEE Access*, *10*, 53015–53026.

Saeedi, K. (2019). Machine Learning for Ddos Detection in Packet Core Network for IoT. Master's Thesis, Luleå University of Technology, Luleå, Sweden.

Sahingoz, O. K., Buber, E., Demir, O., & Diri, B. (2019). Machine learning based phishing detection from URLs. *Expert Systems with Applications*, *117*, 345-357.

Salem, O.; Alsubhi, K.; Shaafi, A.; Gheryani, M.; Mehaoua, A.; Boutaba, R. (2022). Man-in-the-Middle Attack Mitigation in Internet of Medical Things. *IEEE Trans. Ind. Inform. 18*, 2053–2062.

Shaikh, H.; Khan, M.S.; Mahar, Z.A.; Anwar, M.; Raza, A.; Shah, A. (2019). A conceptual framework for determining acceptance of internet of things (IoT) in higher education institutions of Pakistan. In Proceedings of the 2019 International Conference on Information Science and Communication Technology (ICISCT), Karachi, Pakistan, pp. 1–5.

Tahir Ullah, K. (2019). Internet of Things (IOT) systems and its security challenges. *Int. J. Adv. Res. Comput. Eng. Technol*, *8*, 12.

ur Rehman, S.; Khaliq, M.; Imtiaz, S.I.; Rasool, A.; Shafiq, M.; Javed, A.R.; Jalil, Z.; Bashir, A.K.(2021). Diddos: An approach for detection and identification of distributed denial of service (ddos) cyberattacks using gated recurrent units (gru). *Future Gener. Comput. Syst.*, *118*, 453–466.

Wang, Y.; Wang, W.; Ahmad, I.; Tag-Eldin, E. (2022). Multi-Objective Quantum-Inspired Seagull Optimization Algorithm. *Electronics*, *11*, 1834.

Yan, W. (2022). Security Optimization Management for loT-Assisted Bank Liquidity Risk Emergency Using Big Data Analytic-Based Case Reasoning. *Wirel. Commun. Mob. Comput,* 8396931.

Zachos, G.; Essop, I.; Mantas, G.; Porfyrakis, K.; Ribeiro, J.C. (2021). An Anomaly-Based Intrusion Detection System Internet of Medical Things Networks. *Electronics*, *10*, 2562.