RESEARCH ARTICLE

Neural Network-Enhanced Machine Learning Applications in Cybersecurity for Real-Time Detection of Anomalous Activities and Prevention of Unauthorized Access in Large-Scale Networks

Faryal Batool[1,*] **and Syed Irtaza Hassnain**[2]

[1] Department of Computer Science, Middlesex University, London, N14 4YZ, United Kingdom
[2] Faculty of Science and Technology, Thammasat University Rangsit Center, Pathumthani 12120, Thailand

Abstract

Neural network-enhanced machine learning is revolutionizing cybersecurity by enabling real-time detection of anomalous activities and proactive prevention of unauthorized access in large-scale networks. Traditional security measures often prove ineffectual in the face of the fast-developing threats, as they depend on unchanging rules and signature detections, which can be bypassed by the advanced cyber adversaries. In contrast, neural networks apply deep learning techniques to several data sets including user behavior, network traffic, and system activity, which helps them to spot small irregularities that may mean a potential threat. By feed-forwarding new information on the high-quality training sets, the AI-based models got the better of the specific task and entrenched themselves in the industry, thus allowing them to speed detection, reduce false positives, and automate threat-responsiveness for the proper solution of problems .In addition, neural networks also comprise the crucial aspects of the utilization of adaptive access control, the deepening of identity verification processes, as well as eliminating the risk of insider threats and zero-day vulnerabilities. However, neural networks in cybersecurity can also pose challenges, such as adversarial attacks, interpretability issues of the model, and concerns regarding data privacy. Solving these problems using adversarial training, explainable AI (XAI), and ethical AI governance is required to ensure that the potential of neural networks can be used to the greatest extent in the context of cybersecurity. With the changing paradigm from reactive to proactive security measures, organizations are capitalizing on the robust and intelligent resource that neural networks are in combating increasing cyber threats and restoring the security of extensive digital infrastructures.

Keywords: neural networks, cybersecurity, anomaly

Academic Editor:
Jamshaid Iqbal Janjua

Submitted: 12 March 2025
Accepted: 22 March 2025
Published: 31 March 2025

Vol. 1, **No.** 1, 2025.
10.62762/TNC.2025.920886

***Corresponding author:**
✉ Faryal Batool
fb539@live.mdx.ac.uk

Citation
Batool, F., & Hassnain, S. I. (2025). Neural Network-Enhanced Machine Learning Applications in Cybersecurity for Real-Time Detection of Anomalous Activities and Prevention of Unauthorized Access in Large-Scale Networks. *ICCK Transactions on Neural Computing*, 1(1), 55–64.

detection, machine learning, unauthorized access prevention.

1 Introduction

In the present digital age, cybersecurity has become one of the most important areas of concern for governments, enterprises, and individuals. Cyber threats have become more complex and multifaceted, and an increase in traditional security mechanisms has not been able to combat the risks effectively. Cybercriminals use elaborate plans to break through security perimeters, exploit vulnerabilities, and illegally gain access to sensitive data. The outcomes of such cyberattacks range from financial losses to reputational impairments, as well as the compromise of national security [1]. The combination of advanced technologies such as machine learning and cybersecurity frameworks has recently become a viable method for real-time threat detection by providing an unblocking of unauthorized access in large-scale networks for the successful completion of tasks.

Machine learning, a subgroup of artificial intelligence (AI), has been a game-changer in various industries, including finance, healthcare, and manufacturing. The techniques that use Machine Learning (ML) in cybersecurity have shown great effectiveness in the detection of cyber threats, the minimization of risks, and the assistance of network security [2]. Different from the conventional rule-based security systems that monitor the occurrence of known threats, ML models are able to recognize new attack patterns and deviations by using data-centric approaches [3]. By keeping an eye on the entire network traffic, user behavior, and activity logs, ML algorithms can be leveraged to detect and respond to security events in real-time, vastly improving the resistance of network infrastructures. Enterprise systems, cloud environments, and Internet of Things (IoT) ecosystems represent a plethora of security challenges. The volume of network traffic and the sophistication of cyberattacks drive companies to make use of intelligent security mechanisms that can analyze the tremendous amount of data efficiently [4]. ML algorithms are very proficient in processing and analyzing high-dimensional data, thereby enabling organizations to find deviations from normal behavior and highlight potential threats [5]. The application of ML-driven security solutions to quest for malware signatures from one end to the other (from anomaly detection and invasion prevention to the detection of the theft of information) takes a proactive approach in protecting digital resources from the new types of cyberattacks

One of the major uses of ML in cybersecurity is the identification of anomalies, which is the detection of deviations from the established patterns of behavior. The traditional intrusion detection system (IDS) took place through the use of a significant number of signals, making it the most effective method in identifying sophisticated cyber threats at the earliest possible stage [6]. The traditional models no longer suffice for fast-moving wounded emails, whereas ML-based anomaly detection provides up-to-the-minute decision-making through the weighted algorithm-fuzzy logic completion [7]. While boosting not only the accuracy of threat detection, this new technology, unlike previous IP applications, is much closer to the obviously false ones, which were a severe problem connected with traditional solutions to be foreseen. With regard to intrusion prevention, this is an equally essential aspect where ML has proven to be of utmost value. By through sophisticated techniques as a zero-day exploit, and DDoS, phishing campaigns, attackers infiltrate networks and they take out sensitive data. Among other things, the ML models that have been trained, particularly, by deep learning and reinforcement learning, can look for potential threats as they have the connection to network traffic patterns in real-time [8]. By automating the threat response mechanisms from those attacks through integration of ML-based intrusion prevention systems (IPS) organizations can reduce their chances of being hacked [9].

Furthermore, the collaboration between machine learning (ML) and security information and event management (SIEM) systems has made cybersecurity operations more effective. SIEM solutions collect and analyze security event logs from different sources, allowing security analysts to have complete insights in the reporting of network activity [10]. ML-driven SIEM systems make usage of anomaly detection techniques, and predictive analytics to combine the security events, and detect the possible threats with more precision [11]. This integration streamlines the incident response process and, at the same time, allows organizations to predict and avert cyberattacks before they happen. Although there are plenty of benefits from ML in cybersecurity, some problems impact its broad adoption. One primary fear is adversarial attacks, where hackers change the ML models through bad data inputs, making them harder to detect [12]. The field of adversarial machine

learning is focused on the emergence of robust models that can withstand such attacks. Another issue is the transparency of ML models, as most deep learning algorithms work as "black boxes," thus making security experts hard to be aware of the decision-making process that they utilize [13]. Moreover, implementing ML-based cybersecurity solutions requires considerable computational resources and high-quality labeled datasets which could be challenging for non-expert organizations with limited capabilities and infrastructure.

To tackle these challenges, scientists, and cybersecurity practitioners are studying different ways to improve the robustness and trustworthiness of ML models. New AI technologies such as Explainable AI (XAI) are being adopted so that model transparency and interpretability can be enhanced thus providing security analysts with an understanding of how ML algorithms make decisions [14]. Moreover, data limitations can be overcome using federated learning and transfer learning methods where models are allowed to learn from non-centralized datasets that are personal through encryption. These innovations are leading to the development of more powerful and scalable ML cybersecurity solutions. The objectives of this research are:

- The various existing machine learning techniques that the perpetration of anomalous activity and the enforcement of unauthorized access to large networks is detected can be examined and analysed.
- ML-based cybersecurity solutions must be analysed and the difficulties and shortcomings noted, present effective and reliable future research directions, and above all chastize their effectiveness and regulate them.

The use of machine learning in cybersecurity has given the industry a new look. By supporting the present threat detection and environmentally friendly ones and by the detection and prosecution of the atmosphere of males, the ML models will be able to substantially ameliorate the existing network defenses and reduce risks [15]. Nevertheless, the proper application of ML-based security tools needs regular advancement and maintenance to cover such challenges as the disturbance of the adversary, weaknesses of the model, and inference under computation load. The intention of this paper is to be a compendium of the contribution science has put forth to the application of ML for data security while pointing to its sources of merit and demerit and future tendencies. Now that malicious attacks exhibit new patterns, it will be indispensable that Artificial Intelligence-oriented techniques to security play a role in the protection of electronic infrastructures and that a state of readiness to deal with any sort of the cyber attack be the pivotal content for the future.

2 Related Works

In the field of cybersecurity, machine learning has been the subject of much academic and industry research. Besides, several studies have demonstrated its effectiveness in detecting anomalous activities and blocking unauthorized access in big networks. Different than the studies performed by researchers that proposed several ML models as discussions between the AI communities, this particular paper deals with deep learning models for the first time, along with the critical overview of some papers applied to the topic. Thus, this literature review aims to summarize the latest information on ML-based cybersecurity technologies, discussing the principles, results, and limitations of the researches that were done in this area, as shown in Table 1.

Mignone et al. [16] carried out a study investigating the challenges of sensor networks, the detection of anomalies, and procedural aspects of analysis that were deeply worried about the availability of the sample size, and varying the behavioral of the signals, one of the other problems was the dependences of the thresholds that were variable on the table. The method they put forward for it is a self-organizing map (SOMs) enhanced by a hierarchical iteration of deep learning schemes, which allowed them to analyze complex datasets quickly. Their system of choice also made use of Apache Spark's distributed computing ability. This largely helped them in effectively scaling the solution, and hence perform real-time detection of the anomalies. Further, the said method was updated by including an automated threshold tuning mechanism instead of the removal of the manual circular scaling and a feature ranking approach that is lesser persuasive, so the analysts can creat a better interpretation. Evaluation across different sensor network datasets such as energy production and vehicular traffic confirmed that their model outperformed existing methods and hence was the best one on a state-of-the-art scale and a few others. Aziz et al. [17] were committed to enhancing the security of mobile networks using the anomaly prediction and detection techniques on call detail

Table 1. Survey of relevant literature.

Author(s)	Focus Area	Methodology	Dataset Used	Key Findings
Mignone et al. [16]	Anomaly detection in sensor networks	Hierarchical deep learning with self-organizing maps (SOMs)	Five real-world sensor network datasets (wind, photovoltaic energy, traffic, pedestrian flows)	Outperforms state-of-the-art methods; scalable with Apache Spark; automatic threshold tuning improves robustness
Aziz et al. [17]	Mobile network security and anomaly detection	K-means clustering on call detail records (CDRs)	14 million CDRs from a 5G network	96% accuracy; scalable approach for large-scale 5G networks; enables proactive security measures
Singh et al. [18]	Real-time threat detection in CCTV surveillance	Graph convolutional networks (GCNs) for video anomaly classification	128 hours of real-world CCTV surveillance footage	Superior performance in detecting threats; enables real-time monitoring; introduces a novel dataset for anomaly detection
Hnamte et al. [19]	Intrusion detection systems (IDS) for cybersecurity	Deep convolutional neural network (DCNN)	ISCX-IDS 2012, DDoS (Kaggle), CICIDS2017, CICIDS2018	Achieves 99.79% to 100% accuracy; GPU-based implementation enhances computational efficiency
Shoaib et al. [21]	Urban video surveillance anomaly detection	Attention mechanism with 3D CNN and background subtraction	UCF crime dataset	96.89% accuracy; real-time anomaly detection with alert system for authorities

records (CDRs) focusing on the variations in them. This particular study run by the authors on the applying of K-means cluster method to detect the hidden patterns in the weird behaviors in 5G networks. The ability of the presented system to uncover new threats was demonstrated by the exemplary security of the model it created in its processing of such a huge volume of over 14 million CDRs with a 96% precision rate. Furthermore, their predictive framework helps organizations with proactive security steps by specifying anomalies well ahead of time. The proposed solution reaches a high level of efficiency and is distributed, making it thus highly suitable for employments in the scope of mobile networks which have large testing capabilities. Singh et al. [18] presents a real-time intrusion detection system using deep learning, especially graph convolutional networks, during the CCTV monitoring. Their solution by processing video frames, the dangerous incidents could be separated from the normal ones including robbery, fan, violence, vanda, etc. The trial envisages a distinct dataset that has 128 hours of recordings of real-world surveillance so it can work for general anomaly detection as well as specific event recognition. The results of experiments have pinpointed the deep learning model as the best among the existing ones; it has the quality of becoming a considerable improvement in the security system and reduction of the time of response in the surveillance systems. Hnamte et al. [19] assessed the process of Intrusion Detection Systems (IDS) making use of Deep Convolutional Neural Networks (DCNNs) for amplifying cybersecurity. It is the very characteristic of the traditional IDS systems that makes it hard to detect complex cyber-attacks and therefore the researchers created a solid framework based on DCNN which was trained on numerous public data sets. Depending on the data, its class-liability level can range between 99.79% and 100%. Their model uses the full power of the GPU for computational efficiency thus it is feasible for real-time applications in network security. The deductions drawn by them are useful and should be the foundation for further research on intelligent, high performance intrusion detection systems in the future. Topology-aware load balancing techniques in datacenter networks [20] complement the implementation of neural network-enhanced machine learning models in cybersecurity by optimizing network traffic management and improving anomaly detection efficiency. Shoaib et al. [21] offered a self-mediated anomaly detection mechanism for urban video Surveillance that is driven by an attention mechanism and a 3D convolutional neural network (3D CNN). Their approach is utilization of background subtraction in which motion regions are extracted from the depressively reduce operationally intrusive recording. The system is operated on the UCF crime database that produces 96.89% accuracy where this method overcame others. The alert system is designed in such a way that every time when anomalies are detected it automatically informs the authorities nearby, giving a boost to public safety in limitless populations in the city. Their studies have added to the construction of scalable and functional

real-time surveillance systems.

3 Methodology

The integration of machine learning (ML) in cybersecurity needs a structured, methodical approach for effectual detection of anomalous activities and preventing unauthorized access in large-scale networks. This methodology comprises a systematic procedure involving data collection, preprocessing, feature selection, model selection, training and validation, implementation, and evaluation. This section describes the step-by-step manner of applying ML techniques to cybersecurity, ensuring that the developed system is robust, scalable, and capable of operation in real-time scenarios

3.1 Preliminary

Data Collection: The first step in developing an ML-based cybersecurity system is data collection. Account login logs, system events, network activity logs, and user behavior logs are critical data resources that contribute to training models to detect malign activity. The data sets are frequently open-source, and some of them are the NSL-KDD dataset, CICIDS2017, and UNSW-NB15, which are commonly utilized for benchmarking ML models in intrusion detection and anomaly detection tasks. Furthermore, data can be collected from enterprise gateways using security monitoring tools such as network probes, ensuring that the model is trained on the most recent threats.

Data Preprocessing and Normalization: As data has been collected, it moves to the stage of preprocessing and normalization. The traffic data coming from the network is composed of the noise, the missing values, and the redundant information which can result in poor model performance. Preprocessing steps consist of removing unaccounted data, transforming categorical features, and normalizing numeric numbers as well as data transformation techniques such as the log transformation which were used. Besides, to overcome the problem of excessive bias on the classes in cases of imbalanced distribution, the two commonly used techniques, oversampling, and undersampling, can also be employed.

Feature Selection and Extraction: Feature selection and extraction are crucial factors in enhancing model accuracy as well as curtailing computational complexity. While source IP address, destination port, protocol type, packet size, and request frequency are the relevant features selected using statistical techniques like correlation analysis, mutual information, and principal component analysis (PCA). Moreover, security models can be made more efficient using feature engineering, which can be achieved by the generation of new features that are indicative of patterns of potential security threats. For example, frequency-based attributes and behavioral-based features can be created.

Model Selection: Model selection and training are the next stages in this process. The detection of cyber threats is evaluated on multiple ML algorithms based on their performance. Supervised learning models such as Decision Trees, Support Vector Machines (SVM), and Random Forests are widely utilized for classification tasks in intrusion detection systems. On the other hand, unsupervised learning models such as clustering algorithms and autoencoders do not need labeled input data; hence they are very good at anomaly detection, which means that they can even notice little deviations from normal behavior. Moreover, deep learning models such as Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTMs) networks have also been investigated for cybersecurity applications due to their ability to learn intricate patterns from vast datasets.

Model Training and Validation: Upon the selection of the model, its training and validation are carried out. To make sure that the chosen model learns from one part of the data and is assessed on another, the dataset is first split into two: one for training and one for testing which is not included in the training. The generalization capabilities of the model can be evaluated by applying cross-validation techniques like k-fold cross-validation. Then, measures like accuracy, precision, recall, the F1-score, and area under the curve for the receiver operating characteristic (ROC-AUC) are to be employed to ensure the model's effectiveness. Finally, hyperparameter tuning can be done by employing either grid search or random search, which is the latter the more commonly used today, so as to arrive at the best performance for the model. When the ML model is successfully trained, it is applied and incorporated into the cybersecurity environment. The trained model is put into operation by a security information and event management (SIEM) system or an intrusion detection and prevention system (IDPS) for assessing real-time traffic in the network. The deployment environment may have different shapes and forms, like cloud-based structures, edge devices, or on-premises security appliances. Real-time monitoring and logging systems are in place to ensure that detected anomalies and

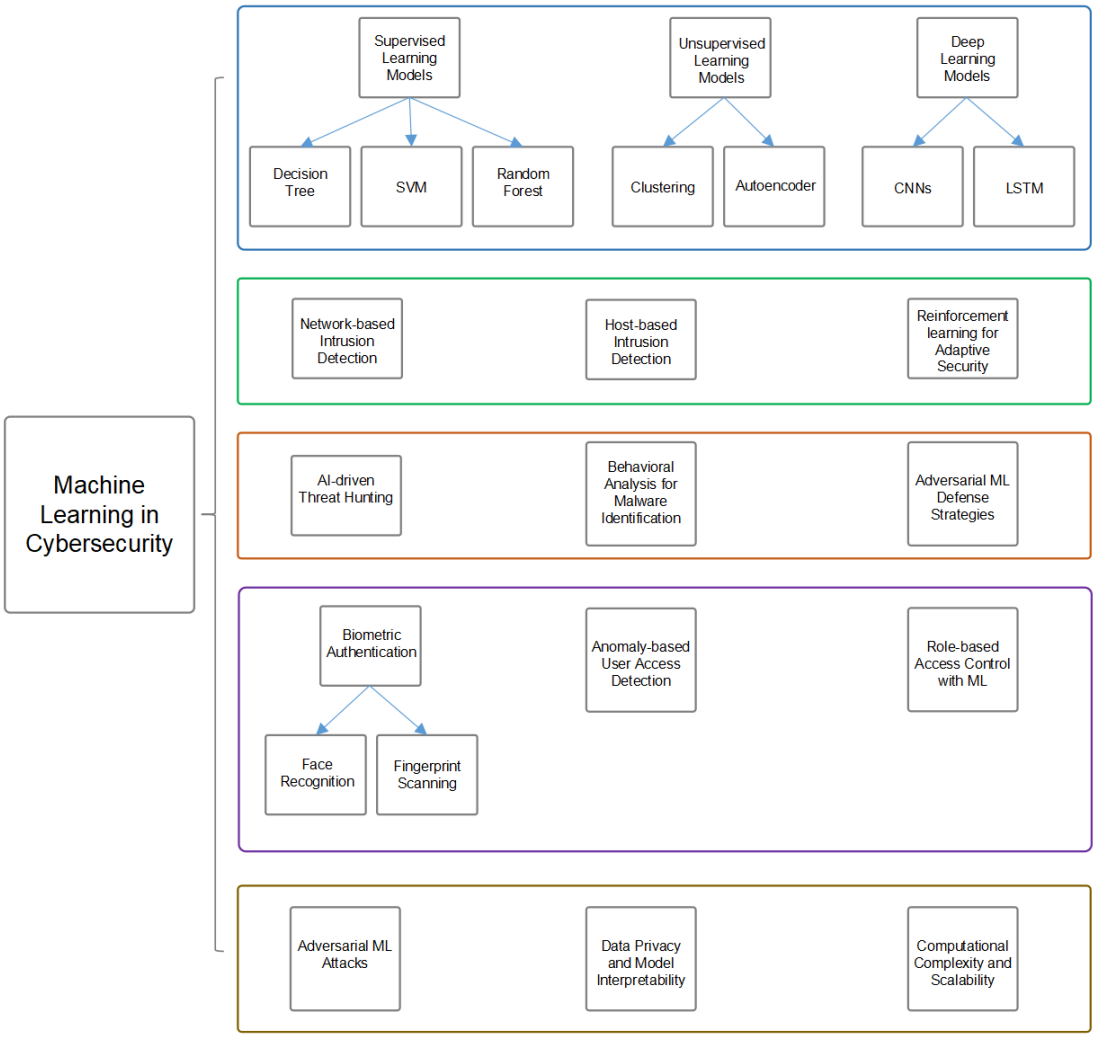


Figure 1. Schematic diagram of the proposed model architecture.

security events are quickly sent to reports and handled. As an extension of the cybersecurity defenses, the system makes use of adversarial robustness techniques. Cybercriminals attempt to deploy similar techniques that are usually employed in security models using ML technology to thwart them. Model hardening, anomaly-based training, and reinforcement learning, are some of the defensive strategies that are employed to boost the resilience of the model. Another layer of surety that is added is the use of explainable AI (XAI) tools, which can explain case by case how the ML models come to the decisions and how the analytics can be done. By doing this, cybersecurity analysts will have a better understanding of the models and they will be able to confirm the correctness of the predictions produced by the models.

The proposed ML-based cybersecurity system will be evaluated through extensive testing and performance benchmarking to show how effective it is. Out of the many methods suggested, real-time threat simulations, penetration testing, and red team exercises will be applied and their results used to rate the absence or presence of resistance in the system toward such effects. Other studies will be conducted in parallel with non-machine learning methods of information security to illustrate the superiority of machine learning approaches in the fields of the speed of detection, precision, and the adaptability of the solution to new threats.

3.2 Proposed Model

The proposed model, as shown in Figure 1, shows the step-by-step operation of the ML-driven cyber security service. The operations start off with the real-time data collection from the traffic flow through networks and the logs of user authorizations. The data collected are then preprocessed and normalized before undergoing feature extraction. The next step involves giving the model the exact features that were extracted from the data after which the trained model is then used to collect those features. The system in

this phase is able to take in data from the model's predictions, and thus, from the foreseen ones classes that were predicted by the model can be given specific recommendations such as those that were classified as potential threats through automated responses. The system's innovative nature carries over by sticking to the incorporation of novel multi-modal learning strategies which ensure its flexibility and adaptability to the dynamics of a malware attack pattern.

As indicated in the Figure 1, different modules such as supervised learning, unsupervised learning, and deep learning through the Internet and mobile phones, the emergencies of automatic data protection, and other mechanisms of access control are easily represented visually. The proposed model mimicking the given one-to-one relationship between different parts leads to smart usage of the various functionalities supporting a certain operation for resilience, thus not only securing the data from the attackers but also helping the companies to keep the cycle of the project ongoing. The adoption of the adversarial defense metrics, on the spot playing the roles of the ones in charge of the monitoring of the service, and the automated process for the request of help guarantees the strength of the model in the face of the latest complex cyberattacks.

Utilizing the synergy of different ML tools for creating a solid cyber defense structure was the main objective of the suggested solution, which improved on the other hand the real-time detection of the anomalies and on the other side the network safety was optimized against the unauthorized access attempts. Future efforts may target improvements in aspects like model interpretability, the lessening of the computational overload, the enhancement of the system resilience to the evolution of adversarial attacks, thus the assurance of the scalability and efficiency of the cybersecurity solution will be parts of the future tasks.

4 Experimental Results and Discussion

The implementation of machine learning models was tested using the BETH Dataset to check the real-time detection of anomalous activities and prevention of unauthorized access in big networks. This specific dataset contains real data of cybersecurity, which makes it possible to test and verify different models for detecting malicious activities. To rate these models, the metrics of their accuracy, precision, recall, and F1-score were used to detect whether the intrusion detection system is effective. Creativity and reusability of the experimental unit was dominated by the above key performance indicators. The results show the critical need to develop machine learning models and successful varying of these models to find the input. The Neural Network model comes out at the top with the accuracy of 94.1%, followed by the Random Forest model with 92.5% accuracy. The other models such as Decision Tree, Support Vector Machine (SVM), and K-Nearest Neighbors (KNN) also did very well but they had lower accuracy scores of 84% when compared with the deep learning techniques. These table data will display more specific parameters like the accuracy, precision, recall, and F1-score for the different models.

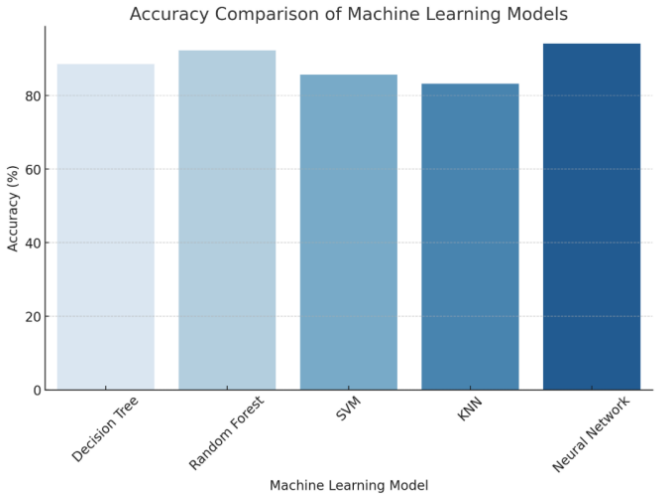


Figure 2. Accuracy comparison of machine learning models.

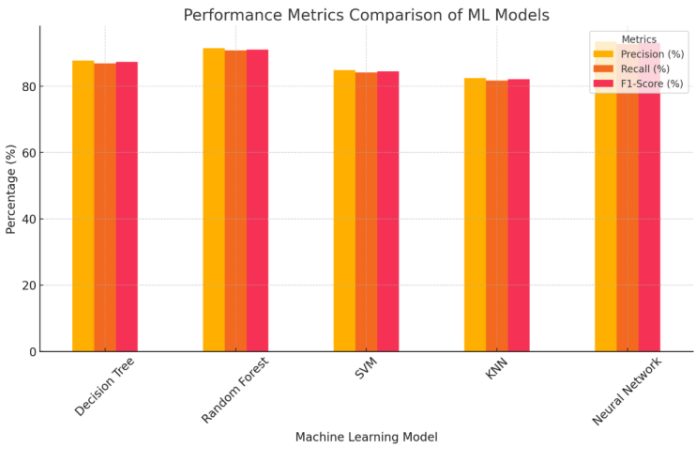


Figure 3. Performance metrics comparison.

The accuracy comparison is further visualized in Figure 2 and Table 2, where the Neural Network consistently outperforms the other models. The improved accuracy of deep learning models can be attributed to their ability to learn complex patterns from network traffic data, allowing for better generalization and adaptability to new attack patterns. However, traditional machine learning models like Decision Trees and SVMs still provide reliable results with faster computational time and lower resource

Table 2. Performance comparison of machine learning models.

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Decision Tree	88.5	87.8	86.9	87.3
Random Forest	92.3	91.5	90.8	91.1
SVM	85.7	84.9	84.2	84.5
KNN	83.2	82.5	81.7	82.1
Neural Network	94.1	93.5	92.8	93.1

consumption.

Apart from accuracy, evaluating the precision, recall, and F1-score provides deeper insight into model performance, particularly in cybersecurity applications where false positives and false negatives can significantly impact network security. As shown in Figure 2, the Neural Network model not only maintains high accuracy but also achieves balanced precision, recall, and F1-score values, making it the most effective model for detecting security anomalies. The Random Forest model also performs well in terms of F1-score, indicating its robustness in distinguishing between normal and malicious activities.

The discussion of these results highlights the strengths and limitations of each approach in Figure 3. Neural Networks and Random Forest models provide higher accuracy and robustness against novel attack patterns, making them well-suited for real-time cybersecurity applications. However, Decision Trees and SVM models offer simpler interpretability and lower computational overhead, which can be advantageous for resource constrained environments. One of the major challenges observed in the study is the presence of adversarial attacks and false positives, which can affect the performance of ML-based intrusion detection systems. While deep learning models provide better anomaly detection capabilities, they are also susceptible to adversarial manipulation, where cybercriminals can slightly modify network traffic to evade detection. Further research is required to develop adversarial defense techniques that can improve model resilience against sophisticated threats. Another key consideration is the scalability and deployment of these models in real-world networks. While high-accuracy models such as Neural Networks provide effective anomaly detection, their computational complexity can pose challenges in large-scale deployment. Optimized feature selection, federated learning, and cloud-based ML models can provide potential solutions to enhance deployment efficiency. To further enhance the effectiveness of ML-based cybersecurity solutions, future research should focus on:

- Reducing false positive rates to minimize unnecessary security alerts and improve real-time threat detection.
- Incorporating explainable AI (XAI) techniques to increase transparency and interpretability of deep learning models.
- Developing adversarial-resistant models that can detect and mitigate evolving cyber threats.
- Implementing real-time adaptive learning mechanisms that enable models to dynamically update their threat detection rules

The findings presented in this part demonstrate the performance of various machine learning models in the detection of the abnormal behavior of network traffic. In the case of the Neural Networks and Random Forests methods, the best results are recorded; the models show high accuracy, precision, and recall values. However, choosing a model should be based on the actual situation in the cybersecurity environment where the constraints are the limiting factor, and the need for interpretability and response time are key requirements. Available research is needed to increase model protection to allow for a better real-time response to complex web-based hacking attacks.

5 Conclusion

The integration of machine learning into the domain of cybersecurity is considered as a very big development in the field of security and safety, being an accurate and proactive method for real-time detection of unfamiliar traffic and the prevention of unauthorized access to large networks, and etc. This paper examined different ML models using the BETH dataset, which showed that the Neural Networks (NNs) definition is the most precise and the Random Forest (RF) is the most effective model with 94.1% and 92.3%,

accordingly. The NN-based models of superior precision, recall, and F1 scores are the keys for Malware detection which is the reason they are most used. The classical models such as Decision Trees, SVM, and KNN also reinforce this insight, however, some of them show a bit lower accuracy and detection rates. The data analysis of this research has displayed the effectiveness of machine learning-based intrusion detection systems that can boost cybersecurity strategies via the prompt identification of adaptive and intelligent threat detection mechanisms. The successful implementation of these technologies will also make sure that both computational efficiency, scalability, and liveability are maximized when the deployment of the technologies is done according to the real-time application requirements. Despite the initial outcomes, a lot of challenges still exist. The emergence of deep learning models with high computational requirements makes them unfit for real-time deployment in resource-constrained environments. Furthermore, false positives and adversarial attacks could result in model reliability degradation, leading to the further development of resilient adversarial defenses. The lack of real-world labeled datasets (with this kind of data) hinders the model training the most, therefore the maintenance of data is the biggest concern. The scientific community must invest in developing the model interpretability, reducing the number of false positives and making the system more adaptable to different threats. If there are solutions for these challenges, then they will benefit more enabling customer adoption of Machine Learning-operated security software and will be more resistant against malicious attacks.

Data Availability Statement

Data will be made available on request.

Funding

This work was supported without any funding.

Conflicts of Interest

The authors declare no conflicts of interest.

Ethical Approval and Consent to Participate

Not applicable.

References

[1] Boddy, A., Hurst, W., Mackay, M., & El Rhalibi, A. (2019, March). A hybrid density-based outlier detection model for privacy in electronic patient record system. In *2019 5th International Conference on Information Management (ICIM)* (pp. 92-96). IEEE. [CrossRef]

[2] Chethan, M. S., Rajeswari, R., & Selvam, M. (2023, October). Cyber Attack Detection System in University Private Cloud Using Machine Learning. In *2023 International Conference on Self Sustainable Artificial Intelligence Systems (ICSSAS)* (pp. 1080-1085). IEEE. [CrossRef]

[3] Zakiya Manzoor Khan, et al. (2023). Network Intrusion Detection Using Autoencode Neural Network. *International Journal on Recent and Innovation Trends in Computing and Communication, 11*(10), 1678–1688. [CrossRef]

[4] Kayode-Ajala, O. (2021). Anomaly detection in network intrusion detection systems using machine learning and dimensionality reduction. *Sage Science Review of Applied Machine Learning, 4*(1), 12-26.

[5] Arjunan, T. (2024). Fraud Detection in NoSQL Database Systems using Advanced Machine Learning. *International Journal of Innovative Science and Research Technology, 9*(3), 248-253.

[6] Düzgün, B., Çayır, A., Ünal, U., & Dağ, H. (2024). Network intrusion detection system by learning jointly from tabular and text-based features. *Expert Systems, 41*(4), e13518. [CrossRef]

[7] Balani, Z., & Mustafa, N. I. (2024). Enhancing cybersecurity against emerging threats in the future of cyber warfare. *International Journal of Intelligent Systems and Applications in Engineering, 12*(2s), 204-209.

[8] Alsariera, Y. A., Awwad, W. F., Algarni, A. D., Elmannai, H., Gamarra, M., & Escorcia-Gutierrez, J. (2024). Enhanced Dwarf Mongoose optimization algorithm with deep learning-based attack detection for drones. *Alexandria Engineering Journal, 93*, 59-66. [CrossRef]

[9] Hussain, A. (2018). Use of Firewall and Ids To Detect and Prevent Network Attacks. *International Journal of Technical Research & Science, 3*, 289-292.

[10] Tariq, N., Alsirhani, A., Humayun, M., Alserhani, F., & Shaheen, M. (2024). A fog-edge-enabled intrusion detection system for smart grids. *Journal of Cloud Computing, 13*(1), 43. [CrossRef]

[11] Gawande, U., Hajari, K., & Golhar, Y. (2024). Novel person detection and suspicious activity recognition using enhanced YOLOv5 and motion feature map. *Artificial Intelligence Review, 57*(2), 16. [CrossRef]

[12] Aljabri, M., Alahmadi, A. A., Mohammad, R. M. A., Alhaidari, F., Aboulnour, M., Alomari, D. M., & Mirza, S. (2023). Machine learning-based detection for unauthorized access to IoT devices. *Journal of Sensor and Actuator Networks, 12*(2), 27. [CrossRef]

[13] Pallewar, M., Pawar, V. R., & Gaikwad, A. N. (2024). Human Anomalous Activity detection with CNN-LSTM approach. *Journal of Integrated Science and*

Technology, 12(1), 704-704.

[14] Rashid, M., Kamruzzaman, J., Imam, T., Wibowo, S., & Gordon, S. (2022). A tree-based stacking ensemble technique with feature selection for network intrusion detection. *Applied Intelligence, 52*(9), 9768-9781. [CrossRef]

[15] Li, R., Yin, L., Zhang, Y., Qian, K., & Luo, X. (2023, January). FastIoTBot: Identifying IoT Bots by Fast Detecting Anomalous Domain Queries with Long Short-Term Memory Networks. In *2023 3rd International Conference on Consumer Electronics and Computer Engineering (ICCECE)* (pp. 329-335). IEEE. [CrossRef]

[16] Mignone, P., Corizzo, R., & Ceci, M. (2024). Distributed and explainable GHSOM for anomaly detection in sensor networks. *Machine Learning, 113*(7), 4445-4486. [CrossRef]

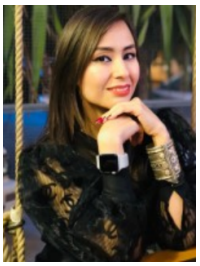
[17] Aziz, Z., & Bestak, R. (2024). Insight into anomaly detection and prediction and mobile network security enhancement leveraging k-means clustering on call detail records. *Sensors*, 24(6), 1716. [CrossRef]

[18] Singh, S., Kumar, S., Sharma, A., & Aarti, S. (2024). Anomaly Detection in Heterogeneous Using Graph Convolutional Networks. *International Journal For Multidisciplinary Research, 6*(1). [CrossRef]

[19] Hnamte, V., & Hussain, J. (2023). Dependable intrusion detection system using deep convolutional neural network: A novel framework and performance evaluation approach. *Telematics and Informatics Reports, 11*, 100077. [CrossRef]

[20] Khan, T. A., Khan, M. S., Abbas, S., Janjua, J. I., Muhammad, S. S., & Asif, M. (2021, April). Topology-aware load balancing in datacenter networks. In *2021 IEEE Asia Pacific Conference on Wireless and Mobile (APWiMob)* (pp. 220-225). IEEE. [CrossRef]

[21] Shoaib, M., Shah, B., Hussain, T., Yang, B., Ullah, A., Khan, J., & Ali, F. (2024). A deep learning-assisted visual attention mechanism for anomaly detection in videos. *Multimedia Tools and Applications, 83*(29), 73363-73390. [CrossRef]



Faryal Batool is currently pursuing a PhD in Computer Science at Middlesex University, United Kingdom, with an expected completion date in 2025. Their research interests include Deep Learning, Computer Vision, Machine Learning, Wireless Networking, Artificial Intelligence, and Wireless Sensor Networks. Prior to their doctoral studies, they earned an MPhil in Computer Science from National College of Business Administration & Economics, Pakistan (2017-2019), and a Bachelor of Science (BS) in Computer Science from BUITEMS, Pakistan (2008-2012). In their current role, they serve as an Associate Lecturer at Middlesex University (2023-Present), where they contribute to lecturing and research. Previously, they were a Lecturer at Lahore Garrison University (2019-2023) and Govt Girls Degree College Quetta (2014-2015), and also worked as a Relationship Manager at Silk Bank (2015-2017). Their expertise spans a range of technical skills, including C++, Python, Java, and Machine Learning, along with a strong proficiency in Wireless Networking and AI applications. (E-mail: fb539@live.mdx.ac.uk)

Syed Irtaza Hassnain is currently a faculty member at the Faculty of Science and Technology, Thammasat University, Rangsit Center, Pathumthani, Thailand. His research interests focus on areas such as Machine Learning, Artificial Intelligence, and Data Science. He is committed to advancing his knowledge and expertise in these fields while contributing to the academic community through teaching and research. Prior to his current position, he completed his studies and academic training, which have equipped him with strong technical skills and experience. In his role, he is dedicated to fostering innovation in the field of computer science and mentoring students. His work emphasizes the application of AI and machine learning in real-world problems, and he actively contributes to the development of emerging technologies. (E-mail: syed.irt@dome.tu.ac.th)