International Journal of Computational and Experimental Science and ENgineering (IJCESEN)

Vol. 11-No.2 (2025) pp. 2838-2848
http://www.ijcesen.com

ISSN: 2149-9144

Research Article

Mobile Network Data Security using Deep Learning

Shilpi Agarwal[1], Sudhir Kumar Sharma[2], Ravi Gupta[3]

[1]Department of ECE & Biomedical Engineering, Jaipur national university, Jaipur, India
*** Corresponding Author Email:** gargshilpi17@gmail.com**- ORCID:** 0009-0002-4774-8617

[2] Department of Mathematics, Bannari Amman Institute Of Technology, Sathyamangalam, Erode, Tamilnadu, India
Email: sudhir.732000@gmail.com **- ORCID**: 0000-0002-8345-3421

[3]Department of Electronics and Communication Engineering, Grace College of Engineering, Thoothukudi, India
Email: raviguptabtp@gmail.com **- ORCID:** 0000-0002-8150-8046

Article Info:

DOI: 10.22399/ijcesen.2295
Received : 20 Fenruary 2025
Accepted : 07 May 2025

Keywords

Mobile Network Security
Intrusion Detection System (IDS)
Anomaly Detection
Network Traffic Analysis
Privacy Protection

Abstract:

With the rapid expansion of mobile networks and the exponential growth of data transmission, ensuring robust security against cyber threats has become a critical challenge. Traditional security mechanisms struggle to keep pace with evolving attack strategies, necessitating intelligent and adaptive solutions. This research explores the application of deep learning techniques to enhance mobile network data security by detecting anomalies, preventing intrusions, and securing communication channels. The study leverages advanced neural network architectures, such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Transformer models, to analyze traffic patterns and identify potential threats in real time. A hybrid deep learning framework is proposed to optimize threat detection efficiency while minimizing false positives. Experimental evaluations on real-world datasets demonstrate significant improvements in accuracy, speed, and resilience against sophisticated cyberattacks compared to conventional security methods. The findings highlight the potential of deep learning-based approaches in strengthening mobile network security, ensuring data integrity, and safeguarding user privacy in an increasingly interconnected digital landscape.

1. Introduction

An effort to breach a company's network security in order to steal sensitive information or carry out some other sort of criminal behaviour is known as a network attack. Any number of external or internal sources might be launching the assault. Data transport and circulation have been enhanced for decades via the use of networking technology. Numerous new services have been made possible by their relentless pursuit of improvement. With the advent of cloud computing, network technology has undergone tremendous changes, allowing for the on-demand provision of various applications, services, computing and storage resources to numerous users over the Internet[1][2]. This model offers numerous benefits, such as adaptability, low administrative burden, efficient use of resources, high accessibility, and reliability.The firewall is a passive defence mechanism against intrusions in conventional system configurations; an intrusion detection system is a sensible, active, and effective addition to it. To detect cyberattacks that might damage information systems, Intrusion Detection Systems (IDSs) are used. Both host-based intrusion detection systems (HIDS) and network intrusion detection systems (NIDS) rely on data analysis to keep networks safe from intrusions. Implementing NIDSs has also made good use of data mining methods, which are effectively used in many other areas. In order to identify cyberattacks, these techniques might unearth intricate connections within the data[3]. Nevertheless, network data cannot be directly processed using commercially available data mining tools. Capturing network data and then preparing and preprocessing it are the first steps in an intricate process that culminates in intrusion detection. Recently, Machine Learning

(ML) and Deep Learning (DL) have become quite popular in the world of network security, and as a result, many new detection methods based on these intelligence techniques are being created all the time to find assaults more rapidly and effectively[4].

Data collection

Data gathering is the first step in the attack detection process. Multiple sites may be used to collect data on network activities. Raw packets and flow records are two forms of data that network devices may offer. Network equipment, such as routers and switches, can usually see what data is coming into and going out of the computers linked to them farther down the chain in a hierarchical (tree) structure. All data packets destined for and arriving at lower-level computers and network devices are visible to higher-level devices, also known as root or core. Horizontal communications, however, are not fully visible to them. These are communications between computers that are on the same level. For aggregation and access devices, which are lower level, the inverse is true. Therefore, the network coverage of an NIDS, the amount of traffic that can be analysed, and the set of cyber-attacks that may be identified are all affected by the choice of the level at which the traffic captures are carried out[5]. There is a great deal of network element traffic in the data collected from root network nodes. If as many network-connected computers as feasible could be targeted by traffic captures at this level, it would be able to identify assaults linked to the Internet. The fact that harmful activity might go horizontally and not affect the root nodes means that certain assaults could go unnoticed. In order to avoid rejecting traffic and minimise detection delays, NIDSs that use root level captures need very high throughput and the ability to handle massive amounts of data[6]. Additionally, they are susceptible to noise and disturbances, such as the addition of a new device to any part of the network, because of the vast number of network parts they include. An essential part of machine learning is feature engineering. In conjunction with ML or DL methods, feature engineering in the sense of feature extraction and feature selection has been implemented. Isolating important data, drawing attention to trends, and enlisting the help of someone with domain knowledge are all steps in improving prediction models[7].

Data preprocessing

To improve the ML models' training process, data processing is a crucial first step. Anyone may access and download any dataset for academic study. Reducing storage space and avoiding redundancy involves removing duplicate samples (flows). To further prevent prediction bias towards the attacker's or victim's end nodes/application, we remove flow indicators like source/destination IP, ports, and timestamps. Next, a categorical encoding method is used to convert the strings and non-numerical attributes into numerical values[8,11]. The ML models are optimised for numerical values, however these datasets include elements like protocols and services that are gathered in their native text values. When it comes to encoding the features, two methods stand out: Hot encoding and label encoding are two methods. To make sure the dataset is free of superfluous data and produces better performance outcomes, transformation and normalisation procedures were applied to it. Feature vectors extracted from the collected traffic data are transformed during the preprocessing step. The end result is a collection of organised records that each detail a distinct traffic observation (packet, connection, session) using a set of factors that may be used for prediction or explanation[8][9]. The goal of the preparation methods is to construct a "clean" dataset by constructing new features, modifying existing ones, and removing noisy samples[12,13].

Network Attack Detection And Prevention Techniques

Network attacks may be detected, defended against, and recovered from with the use of security and defence systems. Security solutions for networks primarily attempt to provide confidentiality, availability, and integrity. The methods used to identify and stop intrusions into networks may be categorised according to whether they focus on prevention or detection. Methods like this may be created in software, hardware, or hybrid forms. One group includes intrusion prevention systems, while the other is intrusion detection systems[10].

Intrusion Detection System (IDS): Also known as Network-based Intrusion Detection Systems (NIDS). Without the ability to prevent attacks, this system diligently watches for malicious network activity and alerts authorities if one is found. IDS primarily employs two methods—signature-based detection and anomaly-based detection—to identify potential threats. By using a database with a set of pre-existing features of known attacks (attacks signatures), signature based methods may identify suspicious occurrences and only discover known threats. New assaults are always being added to the

database, therefore it requires constant maintenance[11]. In contrast, anomaly-based techniques may identify previously unseen dangers by attempting to distinguish between legitimate and malicious network traffic based on observed changes. Abnormal system performance, unusually large traffic, unusual port traffic, or network latency are all signs of deviations from the system's usual behaviour and might be an indication of a network assault.

This system is also known as an intrusion detection and prevention system (IDPS) or an intrusion prevention system (IPS). It constantly checks the network for any suspicious activity that might indicate the existence of rogue control points or unlawful traffic. In order to protect itself from potential dangers, the system takes action automatically. Protecting against harmful or unwanted packets and assaults is the main goal of an intrusion detection and prevention system (IDPS). Due to its ability to do more than only identify threats, IDPS outperforms IDS. Both host-based and network-based intrusion detection and prevention systems (IDPS) are in use today. Host-based systems monitor host activities for suspicious events, while network-based systems analyse the protocol of the network to detect and prevent intrusions[14,15].

The field of machine learning has seen tremendous growth in the last few years. Among the many machine learning approaches, deep learning structures build ANNs to mimic the way neurones in the human brain communicate with one another, giving them a unique advantage when faced with challenging challenges[16,17]. This led researchers to use a variety of deep learning techniques for attack detection, which ultimately led to impressive results[16].

Machine Learning Based Network Attack Detection

Within the field of artificial intelligence, there is a sub-domain known as machine learning (ML). It covers a wide range of application disciplines, including computer science, signal processing, and telecommunication[18], and explores the knowledge from the training data. By creating models that can identify trends to anticipate intrusions, ML algorithms may also be used to intrusion detection systems (IDS) for the purpose of behaviour classification as normal or abnormal[7][19].

The management, monitoring, and security of networks from harmful activity are greatly assisted by intrusion detection systems. The increase in variability in network traffic rates. In an effort to circumvent network security measures, the IDS is fooled by the diversity of queries sent across the network[20]. When dealing with data that is both rapidly changing and very diverse, a Big data architecture is used. Easy tools for acquiring, injecting, preprocessing, storing, analysing, and visualising high-dimensional data are provided[21].

There are three different kinds of ML—supervised, unsupervised, and semi-supervised—that may be used to address security issues. In supervised learning, labels are applied to the training data. All of the inputs and their corresponding outputs are recorded. To do this, we must first train a model to predict or categorise incoming data using labelled inputs. Regression and classification are the two main categories of supervised algorithms[22][23]. Continuous variables may have their future values predicted using regression, which takes past values as input. However, data is divided into distinct groups by classification, which is used for the prediction of discrete variables. Support Vector Machine (SVM), Decision Tree (DT), Random Forest (RF), Naïve Bayes (NB), and Artificial Neural Network (ANN) are some examples of methods that may be used for regression and classification. Since human interaction is required to label the data, the training data for unsupervised learning are not labelled. It is not always simple to label the data. By comparing their levels of similarity, this technique sorts the data into separate clusters. Some examples of these strategies include K-means, K-Nearest Neighbour (KNN), and Self-organising Map (SOM). It is simple to get unlabelled data. Having said that, their use is severely limited. A solution has been developed using semi-supervised learning, which uses both labelled and unlabelled data to construct a more accurate classification model. Theoretically and pragmatically, semi-supervised learning stands out due to the reduced need for human interaction and improved accuracy it offers. Support Vector Machines (SVMs), Decision Trees (DTs), K-Nearest Neighbours (K-NNs), and models based on neural networks are some of the machine learning techniques that have been suggested for use on the scalable framework that makes use of Apache Spark. These models are used to identify breaches in the Big Data Ecosystem (BDE). When dealing with issues with two classes, the models consistently provide excellent solutions across all datasets[24][25]. The detection accuracy falls short for minority classes in multi-class issues, however. The training data was skewed in favour of the majority class, which led to the model's bias. With the abundance of accessible training data, a versatile and effective intrusion detection system (IDS) capable of detecting advanced threats may be best designed using a deep learning technique. Recent years have seen remarkable success for many different types of issues solved using Deep

Learning (DL) techniques across almost all industries[26].

Deep Learning Based Attack Detection

Deep learning, sometimes called hierarchical or deep structural learning, is a method for optimising and self-training models. The efficiency of the learning procedure is enhanced in direct proportion to the amount of data. In comparison to other machine learning methods, it often requires a larger quantity of training data. The hidden layers may be adjusted to meet specific needs, and there are other possibilities to enhance the learning process. In order to improve attack detection systems, it may be beneficial to use various deep learning algorithms. The abundance of information supplied by manually labelled samples allows supervised learning-based systems to often provide high accuracy. Unsupervised learning-based algorithms often perform poorly when there is insufficient information from labelled data. Yet, tagging by hand is a tedious process, particularly when dealing with sophisticated threats. Because actual network assaults are inherently complicated, there are certain instances that defy easy categorization[27]. Thus, it is clear that approaches based on unsupervised learning might do well even without knowing about assaults beforehand. By reducing the amount of training samples while maintaining relatively high performance, hybrid approaches are well-suited to handle diverse attack scenarios. Nevertheless, its extensive use is limited by its typically intricate structure and high computational requirements. Since DNN and CNN outputs solely take into account the influence of the current input, without considering information from the past or future, they are able to accomplish remarkable performance on recognition or classification tasks without time-varying characteristics, making them an ideal choice for attack detection methods based on recurrent neural networks[4,7]. A new class of neural network structures called RNN is suggested for use with time-dependent input; these networks are built with a "memory" function that keeps past information intact. The concept that "human cognition is based on the past experience and memory" is really congruent with this design element. Therefore, RNN excels at processing data that is presented as a time series. Still, RNNs have a few design flaws, such as gradient disappearance or gradient explosion, which causes them to forget or misrepresent long-term dependencies. Thus, LSTM and GRU with gates design and memory cell were developed by researchers. These models effectively maintain long-term relationships by including crucial components of information flow.

2. Literature Review

Author(s)	Year	Approach	Dataset(s)	Key Findings
Rehman et al.	2021	GRU-based DDoS detection (DIDDOS)	CICDDoS2019	99.69% accuracy for reflection attacks, 99.94% for exploitation attacks
Yuan et al.	2021	Parallel Joint Neural Network (CapsNet + Ind RNN)	Not specified	Accuracy: 99.78%, Recall: 99.98%, surpassing traditional models
Yang et al.	2021	ResNet-based malicious traffic detection with DQN and DCGAN	Not specified	Achieved 99.94% accuracy in detecting encrypted malicious traffic
Hussain et al.	2021	CNN-based botnet-coordinated DDoS detection	Real network data	Early detection of CPS-targeted botnet attacks (e.g., SMS spamming, signaling attacks)
Khan et al.	2021	CNN-based NIDS using spectrogram images (STFT)	Not specified	2.5%-4% improvement over DL methods, accuracy: 98.75% (7-class classification)
Reddy & Shyam	2020	DBN with Median Fitness-focused Sea Lion Optimization (MFSLnO)	Not specified	Lightweight malicious node mitigation while maintaining normal network behavior

Kim et al.	2020	CNN-based DoS detection using RGB and grayscale intrusion images	KDD dataset	CNN achieved >99% accuracy in binary and multiclass classification
Gamage & Samarabandu	2020	Hierarchical DL-based anomaly detection	KDD 99, NSL-KDD, CIC-IDS2017, CIC-IDS2018	Four DL models trained and assessed: Autoencoder, DBN, FFNN, LSTM
Venkata & Akkalakshmi	2020	ML/DL-based intrusion detection	NSL-KDD	Supervised learning used for attack classification
Devan & Khare	2020	XGBoost-DNN hybrid model	Not specified	Utilized XGBoost for feature selection and DNN with Adam optimizer for classification
Ergen & Kozat	2020	Gradient-based training for LSTM + OC-SVM/SVDD	Not specified	Enhanced SVM-based anomaly detection with DL techniques
Hu et al.	2019	CNN-based user authentication via mouse dynamics	Balabit Mouse Dynamics Challenge dataset	FAR: 2.94%, FRR: 2.28%, high authentication accuracy
Elsherif	2018	Deep RNN-based threat detection	Not specified	Generalized threat detection using RNN to identify both visible and hidden threats

3. Methodology

Due to its rapid growth and spread, the internet is now present in almost every aspect of human life. Over the last several decades, network systems have been essential to a wide range of online services, including social interactions, shopping, education, banking, business transactions, etc. Because network sizes are growing at an exponential rate, detecting intrusions and assaults has become a new issue. A network attack is the illegal acquisition of a company's computer systems or other digital assets [20].

There are two main types of attacks that may occur on a network. There are active and passive attacks going on here. Malicious actors launch passive attacks when they get access to a network and either steal sensitive data or observe it without making any changes. Acts of data harm, such as deletion, encryption, or unauthorised access, are indicative of an active attack. Firewalls are often the first line of security, although they aren't great at preventing attacks. Intrusion Detection Systems (IDS) are a novel kind of network security that protect systems against DDoS and other unapproved external attacks. By spotting malicious activities, Intrusion Detection Systems (IDS) greatly improve the reliability and security of the. Anomaly detection systems (IDS) and signature-based systems (IDS for abuse) are the two most common types of intrusion detection systems (IDS). By keeping tabs on system activity, anomaly detection systems may spot intrusions into computers and networks, which are then classified as either normal or abnormal based on predetermined criteria or heuristics. The abuse detection system takes defining abnormal system activity as a first step in identifying computer assaults; thereafter, all other activities are deemed normal. Applying deep learning and machine learning techniques to intrusion detection systems (IDS) is one area of research that is analysing and extracting meaningful information from data at a quick pace. The non-linear and increasing dimensionality of the data renders machine learning and deep learning incapable of solving problems requiring multiple classifications. This leads many to believe that feature selection is an essential precondition for learning approaches that aim to enhance learning by eliminating irrelevant or redundant features from the input. When it comes to identifying dangerous threats, it is difficult to estimate the pace of advancement in Intrusion Detection System (IDS) methodologies. In order to train IDSs using deep learning, it is crucial to get a reliable dataset, which is not an easy task. You need a dataset[21] to build deep learning models for intrusion detection systems (IDS). Gathering data packets or flows from the internet is the first stage. In Figure 1, we can see the end result of transforming the gathered traffic into a specific data format that includes network-related information.

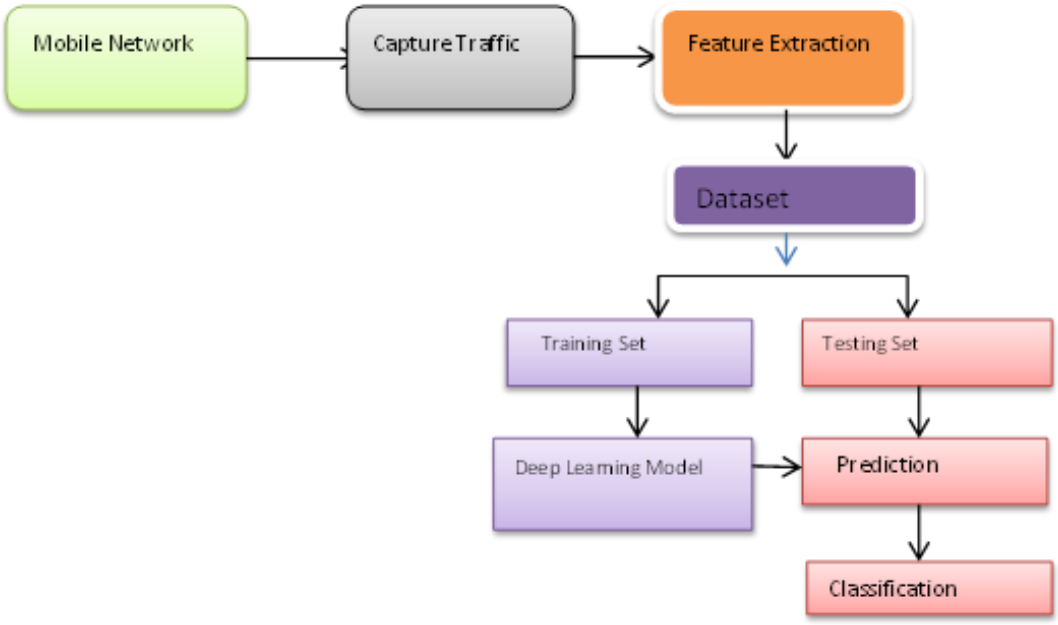

Figure 1. *Deep Leaning based Intrusion detection for Mobile Networks*

Security analysts, incident responders, and network engineers are overwhelmed by the massive amounts of data received and evaluated due to the development of cloud computing, mobile devices, remote workers, networked applications, and global organisations. Nearly half of the businesses surveyed admitted to collecting more data than they could manage from their networks in order to conduct security analyses. The same survey also found that almost half of the companies surveyed had trouble connecting the dots between security breaches and sluggish network performance. Furthermore, cyberattacks are always evolving to be more sophisticated, intricate, and tailored to specific individuals. Security monitoring and incident response rely on data collection, processing, and analysis to identify and mitigate network breaches, despite these complexities. Depending on the need for training, testing, detection, or incident response, various kinds of data may be selected for network analysis from the various components of the network as well as from internal and external hosts. It is already challenging to collect and assess data on network traffic; finding an effective and precise way to do so, and then figuring out how to store and organise the data, adds much more difficulties[13].

Attack detection and prevention firewalls, or stateful firewalls, scan incoming network traffic for malicious indicators and prevent attacks before they occur. There are two ways in which a network or its resources might be "exploited": either to gather information by probing the network or to disable, compromise, or harm it via an assault. Modern, prosperous companies depend on safe networks, yet the truth is that every computer system includes vulnerabilities that are difficult to repair and expensive to disclose.

Business IT systems collect a wealth of data, including internal network traffic, user activity inside the system, different types of connection requests, and much more. Data like this may show questionable or even harmful activity after or even before a large assault, even if most network traffic is innocuous and typical. It may take some time for most teams to react properly following an intrusion event, and the damage and expenditures may quickly add up. Consequently, advanced intrusion detection systems (IDSs) are crucial for the timely and accurate identification of potentially dangerous actions.

A network-based intrusion detection system allows organisations to monitor their cloud, on-premise, or hybrid environments for any suspicious behaviour that may indicate a breach has taken place. Policy violations, port scanning, and traffic from unknown sources all come under this heading. More so than "active" security systems, NIDS are more of a "passive" option. Since their primary function is to alert users of questionable activity, they are often used in tandem with "active" Intrusion Prevention Systems (IPS). Adaptive intrusion detection systems (IDS) may learn to recognise both known and new network behavioural features with the use of Deep Learning, sometimes called Deep Neural Networks (DNNs). This allows them to evict the attacker and reduce the risk of penetration. Anomaly detection, also known as outlier identification, has been the subject of intense study for many years. This is due to the vast array of vital

domains it affects, which include security, compliance, health, medical risk, and the safety of artificial intelligence (AI). Although anomaly identification has been a hotspot for study for quite some time, many problems remain unanswered due to the intricate and one-of-a-kind character of anomalies. There are a number of factors that contribute to the rarity of anomalies in data instances, the fact that their existence is unknown until they happen, the diversity of anomaly types (such as point, contextual, and group anomalies), and the fact that different anomalies exhibit entirely different abnormal characteristics.

4. Results

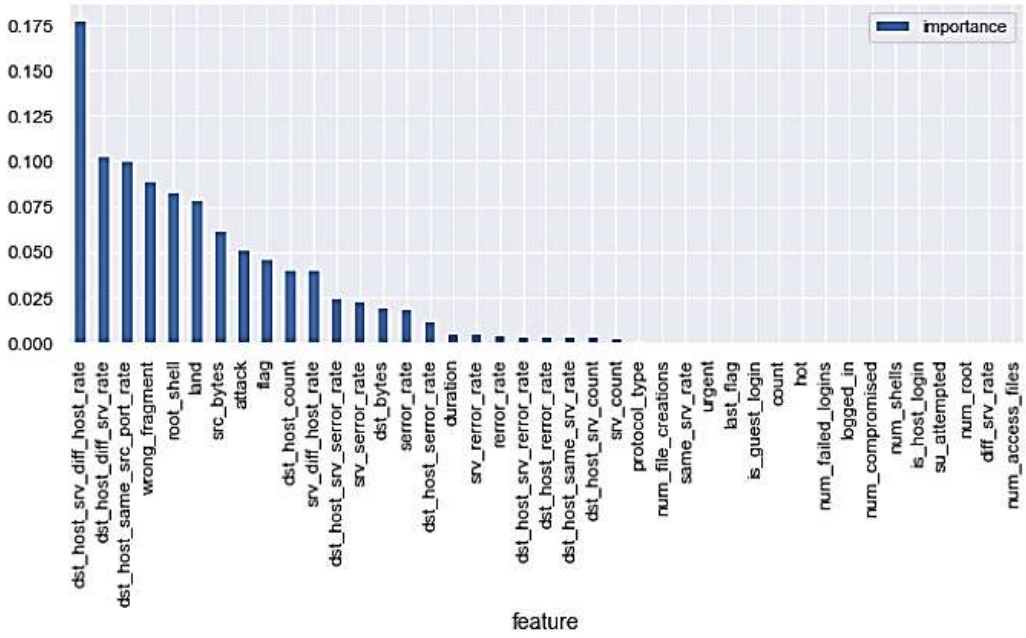

***Figure 2**. feature selection algorithm*

Random Forest Classifier Classification Report

===CLASSIFICATION REPORT===

	precision	recall	f1-score	support
DNS	0.82	0.07	0.13	197
auth	0.64	0.27	0.38	368
browsing	0.99	0.95	0.97	4034
error_reports	0.99	1.00	0.99	815
file_transfer	0.92	0.71	0.80	943
kerberos	0.00	0.00	0.00	67
mail	0.93	0.70	0.80	1074
media	0.99	0.95	0.97	991
netbios	1.00	0.01	0.02	123
oracle	0.00	0.00	0.00	27
others	0.84	0.75	0.80	563
private	0.48	0.95	0.63	2179
remote_jobs	0.00	0.00	0.00	165
search	0.50	0.01	0.01	146
telnet	0.63	0.37	0.46	263
text_services	0.78	0.25	0.38	85
time	0.86	0.21	0.34	142
unix	0.36	0.15	0.21	354
virtual_network	0.00	0.00	0.00	62
accuracy			0.78	12598
macro avg	0.62	0.39	0.42	12598
weighted avg	0.81	0.78	0.76	12598

***Figure 3.** Random Forest Classifier Classification Report with Precision,Recall,F-score,Support*

CONFUSION MATRIX

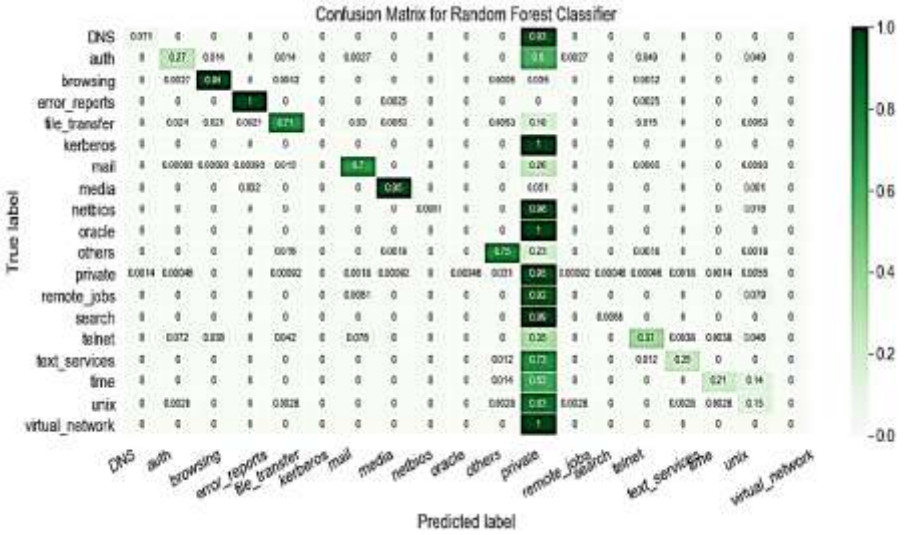

Figure 4.*Confusion Matrix for Random Forest Classifier*

AdaBoost Classifier

	precision	recall	f1-score	support
DNS	0.00	0.00	0.00	151
auth	0.21	0.34	0.26	259
browsing	0.96	0.95	0.96	7889
error_reports	0.62	0.93	0.74	1043
file_transfer	0.30	0.26	0.28	1596
kerberos	0.00	0.00	0.00	45
mail	0.77	0.41	0.54	2417
media	0.52	0.95	0.67	926
netbios	0.00	0.00	0.00	76
oracle	0.00	0.00	0.00	18
others	0.37	0.23	0.28	941
private	0.69	0.77	0.73	4774
remote_jobs	0.00	0.00	0.00	259
search	0.00	0.00	0.00	79
telnet	0.36	0.38	0.37	1668
text_services	0.19	0.19	0.19	54
time	0.12	0.19	0.15	74
unix	0.21	0.37	0.27	232
virtual_network	0.00	0.00	0.00	43
accuracy			0.69	22544
macro avg	0.28	0.31	0.29	22544
weighted avg	0.68	0.69	0.67	22544

Figure 5. *Classification Report for AdaBoost Classifier*

Figure 6. *Confusion Matrix for Adaboost Classifier*

C4.5 Classifier

---CLASSIFICATION REPORT---

	precision	recall	f1-score	support
DNS	0.93	0.07	0.12	197
auth	0.63	0.27	0.37	368
browsing	0.99	0.95	0.97	4034
error_reports	0.99	1.00	0.99	815
file_transfer	0.89	0.70	0.78	943
kerberos	0.00	0.00	0.00	67
mail	0.93	0.69	0.79	1074
media	0.99	0.94	0.96	991
netbios	0.00	0.00	0.00	123
oracle	0.00	0.00	0.00	27
others	0.83	0.75	0.79	563
private	0.48	0.96	0.64	2179
remote_jobs	0.00	0.00	0.00	165
search	1.00	0.01	0.01	146
telnet	0.56	0.33	0.42	263
text_services	0.86	0.22	0.36	85
time	1.00	0.22	0.36	142
unix	0.37	0.15	0.21	354
virtual_network	0.00	0.00	0.00	62
accuracy			0.78	12598
macro avg	0.60	0.38	0.41	12598
weighted avg	0.81	0.78	0.76	12598

Figure 7.*Classification Report of C4.5 Classifier*

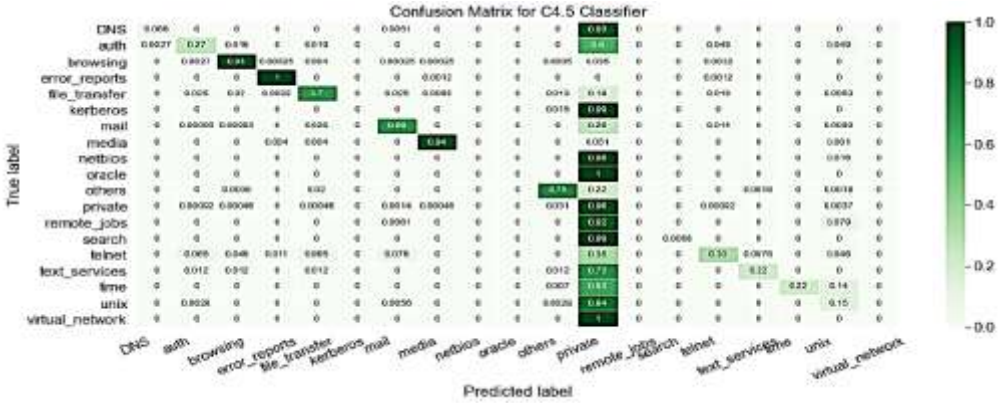

Figure 8.*Confusion Matrix for C4.5 Classifier*

---CLASSIFICATION REPORT---

	precision	recall	f1-score	support
DNS	0.00	0.00	0.00	197
auth	0.00	0.00	0.00	368
browsing	0.32	1.00	0.49	4034
error_reports	0.00	0.00	0.00	815
file_transfer	0.97	0.04	0.07	943
kerberos	0.00	0.00	0.00	67
mail	0.00	0.00	0.00	1074
media	0.00	0.00	0.00	991
netbios	0.00	0.00	0.00	123
oracle	0.00	0.00	0.00	27
others	0.00	0.00	0.00	563
private	0.00	0.00	0.00	2179
remote_jobs	0.00	0.00	0.00	165
search	0.00	0.00	0.00	146
telnet	0.00	0.00	0.00	263
text_services	0.00	0.00	0.00	85
time	0.00	0.00	0.00	142
unix	0.33	0.00	0.01	354
virtual_network	0.00	0.00	0.00	62
accuracy			0.32	12598
macro avg	0.09	0.05	0.03	12598
weighted avg	0.19	0.32	0.16	12598

Figure 9*.Classification Report of SVM Classifier with Precision,Recall,f1-Score,Support*

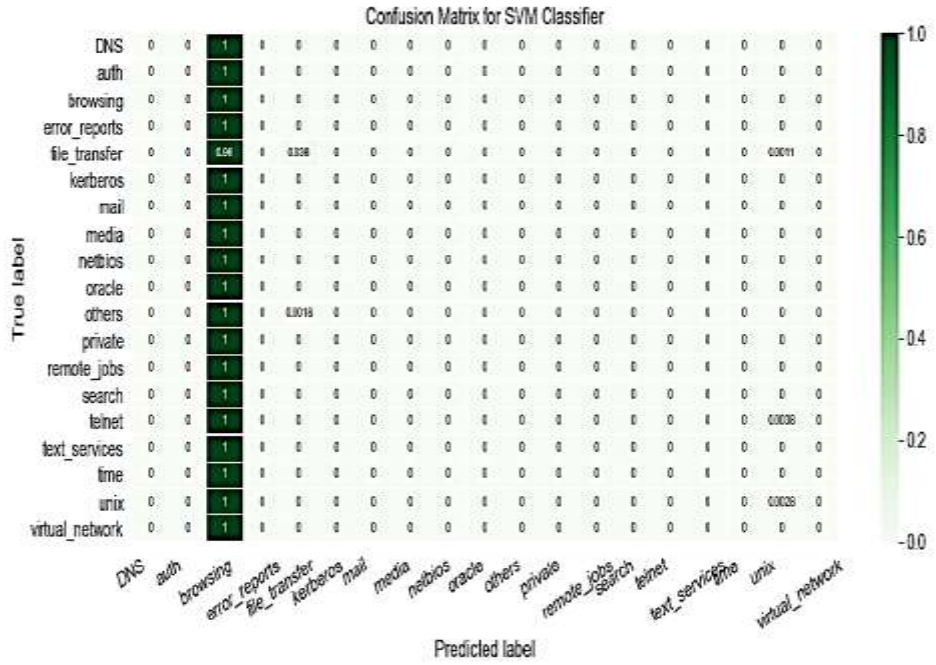

Figure 10. *Confusion Matrix for SVM Classifier*

5. Conclusion

Mobile network security is a critical concern in the era of increasing digital connectivity and cyber threats. This research highlights the potential of deep learning-based solutions in enhancing the security of mobile networks by detecting anomalies, preventing intrusions, and safeguarding user data. By leveraging advanced neural network architectures such as CNNs, RNNs,SVM and Transformer models, the proposed framework effectively identifies malicious activities with high accuracy and minimal false positives. Experimental results demonstrate that deep learning approaches outperform traditional security methods in terms of adaptability, real-time threat detection, and overall network resilience. The integration of AI-driven security mechanisms ensures robust data protection, making mobile communications more secure against evolving cyber threats. Future research can further optimize these models by incorporating federated learning, edge AI, and explainable AI techniques to enhance privacy, efficiency, and interpretability. By continuously advancing deep learning methodologies, mobile network security can evolve to meet the dynamic challenges of the digital landscape, ensuring a safer and more reliable communication ecosystem.

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

[1] Rehman, S. U., 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 Generation Computer Systems, 118*(2), 453–466.

[2] Yuan, J., Chen, G., Tian, S., & Pei, X. (2021). Malicious URL detection based on a parallel neural joint model. *IEEE Access, 9*, 9464–9472.

[3] Yang, J., Liang, G., Li, B., Wen, G., & Gao, T. (2021). A deep-learning- and reinforcement-learning-based system for encrypted network malicious traffic detection. *Electronics Letters, 57*(9), 363–365.

[4] Hussain, B., Du, Q., Sun, B., & Han, Z. (2021). Deep learning-based DDoS-attack detection for cyber-physical system over 5G network. *IEEE Transactions on Industrial Informatics, 17*(2), 860–870.

[5] Khan, A. S., Ahmad, Z., Abdullah, J., & Ahmad, F. (2021). A spectrogram image-based network anomaly detection system using deep convolutional neural network. *IEEE Access, 9*, 87079–87093.

[6] Reddy, S., & Shyam, G. K. (2020). A machine learning based attack detection and mitigation using a secure SaaS framework. *Journal of King Saud University - Computer and Information Sciences, 34*(7), 4047–4061.

[7] Kim, A., Park, M., & Lee, D. H. (2020). AI-IDS: Application of deep learning to real-time web intrusion detection. *IEEE Access, 8*, 70245–70261.

[8] Gamage, S., & Samarabandu, J. (2020). Deep learning methods in network intrusion detection: A survey and an objective comparison. *Journal of Network and Computer Applications, 169*, 102767.

[9] Venkata, R. B., & Akkalakshmi. (2020). Network intrusion detection using deep learning techniques. *International Journal of Advanced Science and Technology, 29*(6), 8278–8287.

[10] Devan, P., & Khare, N. (2020). An efficient XGBoost-DNN-based classification model for network intrusion detection system. *Neural Computing and Applications, 32*(16), 12499–12514.

[11] Ergen, T., & Kozat, S. S. (2020). Unsupervised anomaly detection with LSTM neural networks. *IEEE Transactions on Neural Networks and Learning Systems, 31*(8), 3127–3140.

[12] Hu, T., Niu, W., Zhang, X., Liu, X., Lu, J., & Liu, Y. (2019). An insider threat detection approach based on mouse dynamics and deep learning. *Security and Communication Networks, 12*(4), 1–12.

[13] Elsherif, A. (2018). Automatic intrusion detection system using deep recurrent neural network paradigm. *Journal of Information Security and Cybercrimes Research, 1*(1), 21–31.

[14] Ali, M. H., Al Mohammed, B. A. D., Ismail, A., & Zolkipli, M. F. (2018). A new intrusion detection system based on fast learning network and particle swarm optimization. *IEEE Access, 6*, 20255–20261.

[15] Aljawarneh, S., Aldwairi, M., & Bani Yassein, M. (2018). Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model. *Journal of Computational Science, 25*, 152–160.

[16] Almseidin, M., Alzubi, M., Kovacs, S., & Alkasassbeh, M. (2017). Evaluation of machine learning algorithms for intrusion detection system. In *2017 IEEE 15th International Symposium on Intelligent Systems and Informatics (SISY)* (pp. 277–282). IEEE.

[17] Azmoodeh, A., Dehghantanha, A., & Choo, K. K. R. (2018). Robust malware detection for internet of (battlefield) things devices using deep eigenspace learning. *IEEE Transactions on Sustainable Computing, 4*(1), 88–95.

[18] Bhatia, M., & Sood, S. K. (2017). A comprehensive health assessment framework to facilitate IoT-assisted smart workouts: A predictive healthcare perspective. *Computers in Industry, 92*, 50–66.

[19] Doshi, R., Apthorpe, N., & Feamster, N. (2018). Machine learning DDoS detection for consumer internet of things devices. In *2018 IEEE Security and Privacy Workshops (SPW)* (pp. 29–35). IEEE.

[20] Hamed, T., Dara, R., & Kremer, S. C. (2018). Network intrusion detection system based on recursive feature addition and bigram technique. *Computers & Security, 73*, 137–155.

[21] Li, D., Deng, L., Lee, M., & Wang, H. (2019). IoT data feature extraction and intrusion detection system for smart cities based on deep migration learning. *International Journal of Information Management, 49*, 533–545.

[22] Mazini, M., Shirazi, B., & Mahdavi, I. (2019). Anomaly network-based intrusion detection system using a reliable hybrid artificial bee colony and AdaBoost algorithms. *Journal of King Saud University - Computer and Information Sciences, 31*(4), 541–553.

[23] Mitrokotsa, A., & Dimitrakakis, C. (2013). Intrusion detection in MANET using classification algorithms: The effects of cost and model selection. *Ad Hoc Networks, 11*(1), 226–237.

[24] Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., Al-Nemrat, A., & Venkatraman, S. (2019). Deep learning approach for intelligent intrusion detection system. *IEEE Access, 7*, 41525–41550.

[25] Wang, H., Cao, Z., & Hong, B. (2019). A network intrusion detection system based on convolutional neural network. *Journal of Intelligent & Fuzzy Systems, Preprint*, 1–15.

[26] Doshi, R., Apthorpe, N., & Feamster, N. (2018). Machine learning DDoS detection for consumer internet of things devices. In *2018 IEEE Security and Privacy Workshops (SPW)* (pp. 29–35). IEEE. [**(Noted: Duplicate of #19)**]

[27] Chawla, A., Lee, B., Fallon, S., & Jacob, P. (2018). Host-based intrusion detection system with combined CNN/RNN model. In *Joint European Conference on Machine Learning and Knowledge Discovery in Databases* (pp. 149–158). Springer.