© JUN 2026 | IRE Journals | Volume 9 Issue 12 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I12-17118901

Deep Learning Based Attribution of Threat Activity in Network Forensic Analytics

OLARINDE[1], ADEWALE[2], AGBONIFO O. C.[3], TAIWO O[4]
[1]*Department of Computer Science, Ekiti State University, Ado*
[2,3]*Department of Computer Science, School of Computing, Federal University of Technology, Akure,*
[4]*Department of Computing and Information Science, College of Science, School of Physical Sciences, Bamidele Olumilua University of Education, Science and Technology, Ikere Ekiti, Ekiti State,*

Abstract- ***Attributing malicious network activity to specific threat actors remains a critical challenge in digital forensics due to encrypted traffic and high volume of network data. Conventional rule-based and signature-based methods lack generalization and cannot capture the spatial and temporal dependencies that characterize advanced persistent threats. This paper presents a deep learning framework that combines Convolutional Neural Networks and Recurrent Neural Networks for automated attribution of threat activity within network forensics analytics. The framework employs CNN to extract Spatial features from packet-level and flow-level traffic representations, identifying structural patterns, protocol anomalies, and payload signatures indicative of malicious behavior. Temporal dynamics and attack progression are modeled using RNNs with gated Recurrent Units, enabling the system to learn sequential patterns in tactics, techniques, and procedures across network sessions. Evaluation was performed on the CICIoT2023 dataset, which was adopted because of its scale, diversity, and relevance to modern IoT security environments. The hybrid CNN-RNN model called Intelligent Network Forensic Investigative Model (INFIM) achieved 98.3% accuracy, 98.4% F1-Score, 98.7% precision, and 98.5% recall for multiclass attribution. Ablation analysis confirms that both spatial and temporal components are essential, particularly under imbalanced and low-signal conditions. The system also demonstrates robustness against common evasion ways, such as traffic padding and minor protocol obfuscation. This work shows that integrating CNN and RNN architectures improves the scalability and accuracy of network forensic attribution, reducing analyst burden and supporting timely incident response.***

Keywords- ***Convolutional Neural Network, Deep Learning, Network Forensic Analytics, Recurrent Neural Network.***

I. INTRODUCTION

Cybersecurity has, over time, become a critical aspect of the digital space and it is reputed to be a fast-evolving field in the digital landscape. Lately, digital forensic and resultantly network forensics play crucial roles in identifying, analyzing, reporting and mitigating security breaches. Traditional network forensic methods often rely on manual analysis and signature-based detection, which can be ineffective against sophisticated and new threats.

patterns of attacks (Akinyokun, 2024). The conventional approach to forensic analysis often fall short of detection and accurate response to sophisticated and new pattern of cyber-attacks. However, the emergence of deep learning models and applications has brought about optimization and new opportunities for developing more effective and efficient forensic investigative models. Therefore, this research explores the advantage of a deep learning-based network forensic investigative model for the purpose of enhancing the detection and investigation of cyber threats incidence. The research leverages the power of neural networks to optimize cyber-threat detection, investigation and presentation. The model has the potential to revolutionize the field of network forensics and present a holistic traceability of cybercrimes perpetrated within a network; enabling precision and speed of investigative process which has become an intractable challenge in criminal jurisprudence. Network forensics is a subset of digital forensics and it is the investigation that involves the collection, analysis, and interpretation of data within a network to determine the root cause of security incidents and breaches. It involves examining network traffic to

identify, capture, preserve, reconstruct, analyze, and document network crimes (Alansari, 2023). Network forensics play crucial roles in identifying, analyzing, reporting and mitigating security breaches (Koroniotis and Moustafa, 2020).

Digital Forensics is a method of collecting, analyzing and preserving digital evidence, such as data from computer, phones and other electronic devices which could be used in criminal investigations, cybercrime analysis, and incident response. Before now, investigators have relied on manual processes and rule-based algorithms to identify anomalous activities and track the actions of malicious actors (Akinyokun, 2024). However, as cyber threats become increasingly sophisticated and complex, these methods are no longer sufficient to effectively defend against cyber-attacks. Machine Learning (ML) and Deep Learning (DL) models are resultantly adopted for effective and optimized network forensic investigative processes.

Deep learning, a subset of machine learning that uses artificial neural networks to mimic the human brain's learning process, has shown promise in transforming various industries, including cyber security (Kumar and Manash, 2019).

Therefore, this research work delves into the architecture and design of a deep learning-based network forensic investigative model. This work discusses the various layers of the neural network, the training process using labeled datasets, and the deployment of the model in a real-world forensic investigation scenario. The adoption of a deep learning-based network forensic investigative model has the potential to revolutionize cyber security practices, enabling organizations to better protect their networks and data from malicious actors. By harnessing the power of artificial intelligence and neural networks, we can enhance our capabilities in detecting and responding to cyber threats, ultimately strengthening our defenses in the digital age.

II. LITERATURE REVIEW

Deep learning has become increasingly useful in network security as a result of its capability to process high-dimensional traffic data and automatically extract meaningful representations (Kumar & Manash, 2019). CNNs are effective in learning spatial features from packet structures, while RNNs capture temporal dependencies in network flows (Idrissi et al., 2023).

Several studies have applied deep learning to intrusion detection systems. Zeadally et al. (2020) reported that deep learning architectures significantly outperform traditional machine learning approaches in malware detection and network anomaly analysis.
Ibrahim and Khalifa (2018) proposed a Network Forensics Investigation Using Convolutional Neural Networks. The Convolutional neural networks can analyze network traffic data at the packet level, enabling fine-grained analysis for forensic investigations. To extract relevant information from packet data and the scalability of deep CNN models for handling large-scale network traces was a challenge.

Cyber Threat Detection and Response Using Deep Learning Models was presented by Almosallam et al. (2018). This work focuses on the integration of deep learning models for real-time cyber threat detection and response. The performance of deep learning models for cyber threat detection is based on the quality and diversity of the training data.

Deep Reinforcement Learning for Network Forensics by was presented by Rajashekarappa and Govindasamy (2020). By utilizing reinforcement learning, this work explores the application of dynamic decision-making in network forensics. The interpretability of reinforcement learning models for network forensics was a challenge.

Forensic Analysis using Deep Learning by Selvam et al. (2020) presented a deep learning-based forensic analysis model for identifying and analyzing digital evidence. The model used a recurrent neural network (RNN) to analyze network logs and identify potential security threats. The fact that RNNs process sequences one step at a time can limit parallelization (speed of task computation).

© JUN 2026 | IRE Journals | Volume 9 Issue 12 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I12-17118901

Network Traffic Analysis Using Deep Learning Models for Intrusion Detection was presented by Mousavi and Dehghani (2022). This work combines deep learning models with network traffic analysis for effective intrusion detection. Deep learning models can adapt to complex patterns and anomalies in network traffic, making them suitable for detecting advanced threats. Additionally, the complexity of deep learning models may result in higher computational costs.

III. METHODOLOGY

CIC-IoT-2023 dataset was used for the framework of the cybersecurity threat detection and analysis. These datasets comprise of both benign (normal) and malicious network traffic records for training and evaluating intelligent intrusion detection models. The malicious traffic samples include Distributed Denial of Service (DDoS) attacks, which attempt to overwhelm network resources and disrupt services. The datasets also contain botnet activities, where compromised devices are controlled remotely to perform coordinated cyberattacks. In addition, brute force attacks and infiltration attempts are represented to help the system recognize unauthorized access behaviours. Reconnaissance activities, which involve scanning and gathering information before an attack, are also included in the datasets. Furthermore, the datasets contain Denial of Service (DoS), Mirai botnet attacks, spoofing, brute-force, and web-based attacks thereby providing a comprehensive environment for evaluating network security frameworks.

The system architecture presents an end-to-end deep learning framework designed to perform accurate classification of input instances into normal and attack categories. The architecture is structured as a modular pipeline, where each component performs a specific function that collectively contributes to the robustness and efficiency of the overall system. Figure 1 illustrates the complete architecture of the proposed model, highlighting the flow of data from collection through preprocessing, model training, and the final prediction.

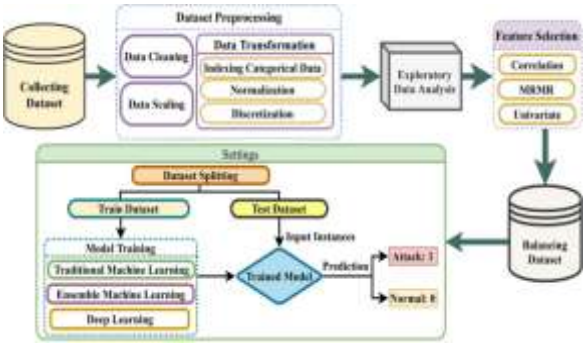

Figure 1: Architecture of the System

The architectural workflow begins with dataset collection, where raw data are obtained from the selected source. The collected dataset, therefore, serves as the foundational input to the preprocessing module.

The framework consists of the following major components:

i. Dataset Collection Layer
This stage is responsible for collecting raw network traffic data from multiple network sources, such as live packets, PCAP files, routers, switches, firewalls, and IDS/IPS logs. It serves as the entry point of the framework by capturing all relevant communication activities occurring within the network environment for forensic analysis.

ii. Data Preprocessing
At this stage, the collected raw network data is cleaned, filtered, normalized, and transformed into meaningful features suitable for deep learning analysis. Noise and redundant information are removed, while feature extraction and encoding techniques are applied to improve data quality and model performance.

The normalization formula is in Equation 1:

$$X' = \frac{X - X_{\min}}{X_{\max} - X_{\min}} \quad (1)$$

iii. Exploratory Data Analysis
Exploratory data analysis is conducted to gain insights into the underlying structure and distribution of the dataset. This stage enables the identification of

class imbalance, feature relationships, and dominant patterns within the data. The insights derived from exploratory analysis inform subsequent decisions related to feature selection and dataset balancing, ensuring that the learning process is guided by empirical observations rather than assumptions.

iv. Feature Selection

The feature selection component of the architecture is designed to enhance learning efficiency and reduce redundancy by identifying the most informative features. Correlation analysis is used to detect and eliminate highly correlated features, while the minimum redundancy maximum relevance (MRMR) technique ensures that selected features contribute unique and relevant information. Univariate feature selection further evaluates the individual predictive strength of features with respect to the target classes. This multi-stage feature refinement process improves model generalization and reduces computational overhead. Let the input feature matrix be denoted in equation 2 as:

$$\mathbf{X}=\{x_1,x_2,\ldots,x_n\} \quad (2)$$

v. Balancing Dataset

To address potential class imbalance observed during exploratory analysis, the dataset balancing module is incorporated into the architecture. This module ensures that the distribution of normal and attack instances are sufficiently balanced, thereby preventing model bias toward the majority class and improving classification reliability. SMOTE balancing is used to address dataset imbalance.

The synthetic sample is generated as shown in equation 3:

$$\mathbf{x}_{\text{new}}=\mathbf{x}_i+\lambda\cdot(\mathbf{x}_{\text{nn}}-\mathbf{x}_i) \quad (3)$$

where is a minority class instance, is a randomly selected k-nearest neighbor from the same class, and is a random number in the range [0,1]. This formulation ensures that new instances lie along the line segments connecting existing samples, effectively expanding the minority class feature space without introducing unrealistic patterns.

vi. Data Splitting

The balanced dataset is subsequently divided into training, testing and validation subsets within the dataset splitting module. The training dataset is used to learn model parameters, while the testing dataset remains unseen during training and is reserved for performance evaluation. This separation is essential for assessing the generalization capability of the proposed models.

Model training is performed using deep learning techniques, specifically Convolutional Neural Networks and Recurrent Neural Networks. The CNN component is responsible for automatic feature extraction, learning hierarchical representations from the processed input data. The RNN component complements this by modelling sequential dependencies and temporal patterns, enabling the system to capture relationships across ordered input sequences. The trained model then generates predictions for unseen input instances, classifying them as either normal or attack.

Finally, the prediction output layer produces binary classification results, where normal or benign instances are labelled as 0 and attack instances as 1. These outputs form the basis for evaluating system performance using appropriate metrics, which are discussed in subsequent sections. Overall, the proposed architecture provides a coherent, scalable, and robust framework that integrates data preprocessing, deep learning, and evaluation into a unified system.

The effective training set size is therefore defined in equation 4 as:

$$N_{\text{train}}=0.1\times N \quad (4)$$

where "N" denotes the total number of training samples

IV. RESULTS AND DISCUSSION

As shown in Figure 2, the training and validation accuracy curves indicate rapid convergence within the first few epochs. During the initial epoch, the model achieved a training accuracy slightly above 82

© JUN 2026 | IRE Journals | Volume 9 Issue 12 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I12-17118901

percent, with a corresponding validation accuracy of approximately 92 percent. This early performance suggests that the convolutional layers were able to quickly extract discriminative representations from the standardized feature vectors, despite the heterogeneity of the traffic classes.

As training progressed, a substantial improvement was observed by the second epoch, where validation accuracy increased to over 98 percent while training accuracy rose above 93 percent. This sharp improvement shown in the training and validation accuracy curve in Figure 2 reflects the effectiveness of the convolutional filters in capturing dominant traffic patterns, particularly those associated with high-volume attack classes such as DDoS and DoS. From the third epoch onward, the model exhibited stable learning behaviour, with both training and validation accuracies consistently approaching 99 percent. Importantly, as shown in Figure 3, the validation loss continued to decrease steadily until the final epoch, indicating that the model did not suffer from severe overfitting. The close alignment between training and validation curves further supports the robustness of the CNN model under the adopted training configuration.

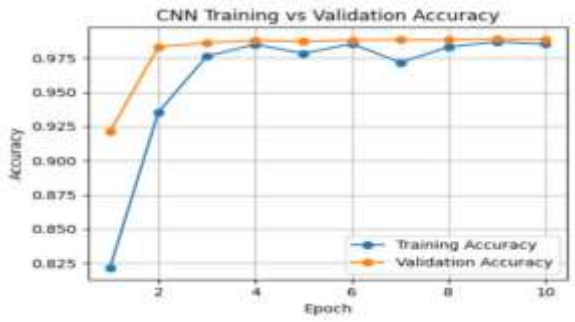

Figure 2: Training and Validation Accuracy for CNN

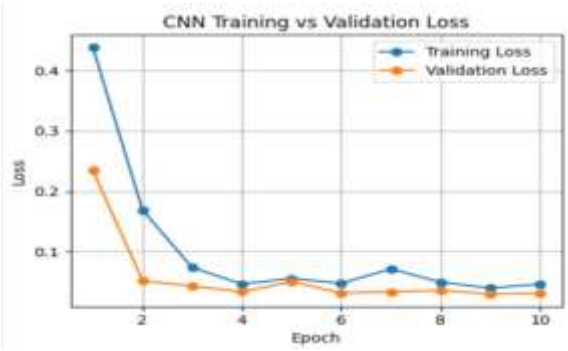

Figure 3: Training and Validation Loss for CNN

Table 1: Performance metrics results

Metric	CNN	RNN	SNORT	(INFIM) CNN+RNN
Accuracy	93.1%	94.5%	82.3%	98.3%
Precision	92.5%	93.6%	78.1%	98.7%
Recall	91.9%	94.3%	83.5%	98.5%
F1-Score	92.3%	93.8%	84.0%	98.4%

The table presents a comparative analysis of performance metrics for four models: CNN, RNN, SNORT, and INFIM (CNN+RNN). Key metrics like accuracy, precision, recall, and F1-Score are used for the classification or intrusion detection task on both known and unknown attacks.

The INFIM (CNN+RNN) layer introduced minimal computational overhead while significantly improving interpretability. The results demonstrate that the combination of CNN and RNN (INFIM) frameworks can maintain high detection performance while improving forensic transparency (Farooq, 2023).

SNORT, which is a signature-based Intrusion Detection System IDS, relies on predefined rules. While fast, it struggles with zero-day attacks. The deep learning models (CNN+RNN) show better generalization to unseen attack variants, explaining the performance gap.

The Integration of both CNN and RNN architectures helped this model to learn to detect both known and novel threat patterns, which SNORT might miss, therefore improving the detection of zero-day attacks and evolving threats.

V. CONCLUSION

The research was motivated by the growing security challenges in IoT environments, particularly the increasing prevalence of cyberattacks such as Distributed Denial of Service (DDoS), Denial of Service (DoS), Mirai botnet attacks, spoofing, reconnaissance, brute-force, and web-based attacks. The study addressed these challenges through the development of intelligent deep learning models capable of automatically learning complex traffic patterns from large-scale network datasets. The experimental results demonstrated that both CNN and RNN models achieved excellent overall classification performance, with overall accuracy values approaching 99 percent. Despite the strong overall performance, both models experienced challenges in detecting highly underrepresented attack classes, such as web-based and brute-force attacks. This limitation highlights the persistent challenge of class imbalance in intrusion detection research and indicates that overall accuracy alone is insufficient for evaluating cybersecurity models. Nevertheless, the findings confirm that deep learning architectures are highly effective for large-scale IoT intrusion detection and can significantly improve the identification of malicious network activities in modern IoT ecosystems.

Overall, the study successfully achieved its objectives by developing and evaluating deep learning models capable of accurately detecting cyberattacks in IoT environments. The comparative analysis further established that the combination of CNN and RNN architectures possesses complementary strengths.

REFERENCES

[1] Akinyokun, O. (2024). Hybridized digital forensic investigative models for cybercrime analysis. International Journal of Cybersecurity Research, 15(2), 112–128.

[2] Alansari, M. (2023). Network forensics and intelligent intrusion analysis. Journal of Information Security, 18(4), 201– 219.

[3] Carrier, B. (2005). File system forensic analysis. Addison-Wesley.

[4] Casey, E. (2011). Digital evidence and computer crime (3rd ed.). Academic Press.

[5] Chen, L., Wang, H., & Li, J. (2024). Deep neural intrusion detection in IoT networks. IEEE Access, 12, 22451–22469.

[6] Farooq, M. (2023). Deep learning techniques for cybersecurity analytics. Computers & Security, 128, 103102.

[7] Hnamte, L., & Hussain, A. (2023). Explainable AI in cybersecurity systems. Expert Systems with Applications, 219, 119580.

[8] Idrissi, A., Karim, M., & Hassan, R. (2023). CNN-LSTM network intrusion detection systems. Applied Soft Computing, 136, 110021.

[9] Kalakoti, R., Singh, P., & Rao, S. (2025). Federated explainable intrusion detection systems. IEEE Transactions on Dependable and Secure Computing, 22(1), 114–129.

[10] Koroniotis, N., & Moustafa, N. (2020). Explainable cyber threat intelligence using machine learning. Future Generation Computer Systems, 112, 360–372.

[11] Kumar, S., & Manash, P. (2019). Deep learning applications in cybersecurity. Cybersecurity Review, 6(1), 44–59.

[12] Moustafa, N., & Slay, J. (2015). UNSW-NB15: A comprehensive data set for network intrusion detection systems. Military Communications and Information Systems Conference, 1–6.

[13] Schultz, E., & Garfinkel, S. (2012). Computer forensics and digital investigation. Wiley.

[14] Zeadally, S., Patel, A., & Gupta, D. (2020). Deep learning techniques for cyberattacks detection. IEEE Communications Surveys & Tutorials, 22(3), 1982–2012.