Campus Network Traffic Prediction and Anomaly Detection Based on Deep Learning

Jun Li[1,2], Noel B . Linsangan [1] and Huiguo Dong [2]
[1]Graduate School, Mapua University, Manila, Philippine
[2]Hebei Vocational University of Technology and Engineering, Hebei, China
nblinsangan@mapua.edu.ph

***Abstract*—This paper proposes an intelligent solution for network traffic prediction and anomaly detection in campus networks, addressing the increasingly severe network security challenges. The proposed approach innovatively integrates Convolutional Neural Networks (CNN) and Long Short-Term Memory networks (LSTM) to simultaneously extract local features and capture dynamic temporal dependencies of network traffic, significantly improving prediction accuracy. Based on this, an adaptive threshold anomaly detection algorithm is designed to automatically adjust detection sensitivity according to traffic variations, achieving a better balance between accuracy and recall rates. Additionally, an anomaly visualization scheme is presented, intuitively displaying the spatiotemporal distribution of network anomalies through heatmaps, assisting administrators in decision-making. Large-scale experiments demonstrate that this approach can effectively identify various security threats such as DDoS attacks, scanning probes, and botnets, with an overall detection rate exceeding 90% while maintaining a low false positive rate. Compared to traditional statistical and machine learning methods, the proposed approach exhibits stronger adaptability and generalization capabilities, providing crucial support for building an intelligent, precise, and reliable campus network security protection system. Future work will focus on further improving the real-time performance and robustness of the solution, expanding its application in new network scenarios such as IoT and edge computing.**

***Index Terms*—Campus Network Security, Network Traffic Prediction, Anomaly Detection, Deep Learning, Visualization**

I. Introduction

As campus networks continue to expand and the increasing richness of applications, network traffic has shown an explosive growth trend [1]. However, the complex and dynamic network environment also provides opportunities for various network security threats, such as denial of service attacks, botnets, and data breaches [2]. Timely and accurate prediction of network traffic changes and detection of abnormal behaviors are crucial for ensuring the secure and stable operation of campus networks [3].

Traditional methods for network traffic prediction and anomaly detection mainly include time series models [4], statistical learning [5], and shallow machine learning [6]. However, these methods often struggle to effectively handle the high-dimensional, non-linear, and dynamic characteristics of network traffic, resulting in limited prediction and detection accuracy [7]. In recent years, artificial intelligence technologies represented by deep learning have made significant progress, demonstrating excellent performance in fields such as image recognition and natural language processing [8]. Introducing deep learning into network traffic analysis and security protection is expected to overcome the limitations of traditional methods and significantly improve prediction and detection effectiveness [9].

This paper proposes an intelligent solution for campus network traffic prediction and anomaly detection based on deep learning. The solution comprehensively utilizes Convolutional Neural Networks (CNN) and Long Short-Term Memory networks (LSTM) to construct an end-to-end hybrid neural network model, capable of simultaneously extracting local features of traffic and capturing long-term dependency relationships, achieving precise traffic prediction. Based on the prediction results, an anomaly detection algorithm with dynamic threshold adjustment is further designed, which can adaptively identify abnormal traffic according to the residual distribution and intuitively present the detection results in the form of heatmaps. In addition, this paper also built a prototype system based on Software-Defined Networking (SDN) to deploy and evaluate the performance of the proposed solution in a real environment. Experimental results show that this solution can significantly improve the traffic prediction accuracy and anomaly detection capability of campus networks, safeguarding the security of smart campus networks.

II. Related Work

Research on network traffic prediction and anomaly detection has a long history, with many different methods proposed by domestic and international scholars. Traditional time series models such as Autoregressive Moving Average (ARMA) [10] and Autoregressive Integrated Moving Average (ARIMA) [11] establish mathematical models to predict future trends through statistical analysis of past traffic. However, these models usually assume that traffic follows specific probability distributions, lacking adaptability to complex real-world scenarios. Statistical learning methods such as Support Vector Machines (SVM) [12] and K-Nearest Neighbors (KNN) [13] achieve classification or regression prediction by constructing statistical discriminative models based on multidimensional features of traffic. However, they mostly adopt shallow structures, making it difficult to fully mine the deep information contained in high-dimensional data. Shallow machine learning methods such as decision trees [14] and naive Bayes [15] overcome some shortcomings of statistical learning to a certain

ISSN:3006-2985(Print)
ISSN:3006-9297(Online)

extent by feature engineering and classification modeling of traffic. However, the process of manually extracting features often relies on expert experience, has limited generalization ability, and struggles to cope with dynamic changes in the network environment.

To address these issues, researchers have begun to introduce deep learning techniques into the field of network traffic analysis. One category of methods focuses on modeling raw traffic using Deep Neural Networks (DNN) or their variants [16], thereby automatically learning high-order abstract features. For example, reference [17] designed a DDoS attack detection model based on Deep Belief Networks (DBN), achieving excellent performance on the KDD Cup 99 dataset. Reference [18] proposed a network anomaly detection framework based on Convolutional-Long Short-Term Memory networks (CNN-LSTM), capable of extracting discriminative representations of traffic from both spatial and temporal dimensions simultaneously. Another category of methods focuses on the fusion of deep learning and traditional machine learning [19], leveraging the complementary advantages of both. For instance, reference [20] combined Stacked Autoencoders (SAE) and Support Vector Data Description (SVDD) to construct a semi-supervised network intrusion detection model, demonstrating good detection performance on the NSL-KDD dataset. Reference [21] ingeniously integrated Long Short-Term Memory networks (LSTM) and Extreme Learning Machines (ELM) to achieve real-time detection and interception of malicious URLs.

Although existing work has made encouraging progress, there are still some urgent issues to be addressed: First, there is a lack of specialized research focusing on campus network scenarios, making it difficult to fully consider their unique traffic patterns and security requirements [22]. Second, most adopt a single deep learning model, neglecting the complementarity of different models in feature extraction and sequence modeling [23]. Third, there is a lack of transparent and credible explanations for detected anomalies, which is not conducive to administrators taking timely countermeasures [24]. This paper attempts to address these shortcomings by proposing an end-to-end solution that integrates multiple models and conducts thorough experimental validation on actual campus networks.

III. End-to-End Intelligent Prediction and Detection Solution

A. Overall Architecture of the Solution

In today's digital campus environment, intelligent prediction of network traffic and anomaly detection have become key tasks for ensuring campus network security and optimizing resource allocation. To address this challenge, the CNN-LSTM hybrid model demonstrates great potential in campus network management due to its powerful sequence data processing capabilities. This deep learning architecture effectively captures spatial and temporal features in network traffic data by combining the advantages of Convolutional Neural Networks (CNN) and Long Short-Term Memory networks (LSTM).

The principle of applying the CNN-LSTM model to campus network traffic analysis can be summarized as follows:

1) **Spatial Feature Extraction:** First, the model uses CNN layers to process raw network traffic data. Through a series of convolution and pooling operations, CNN can identify spatial features in traffic patterns, such as traffic characteristics of specific applications or services, and user behavior patterns.
2) **Feature Transformation:** The multidimensional features extracted by CNN are then flattened into one-dimensional vectors. This step transforms complex network traffic features into a format suitable for temporal analysis.
3) **Temporal Dependency Modeling:** LSTM layers receive these transformed features and model the time series of network traffic. The special structure of LSTM allows it to capture long-term traffic trends and periodic patterns, such as traffic variations during daily routines, weekends, or special events.
4) **Prediction and Detection:** The model's output can be used to predict future network traffic trends or detect abnormal traffic patterns. This can be achieved through additional fully connected layers or specialized output layers to generate final prediction results or anomaly alerts.

The intelligent traffic prediction and anomaly detection solution for campus networks proposed in this paper is shown in Figure 1. The solution takes deep learning as its core, integrating multiple functional modules such as data preprocessing, hybrid neural networks, anomaly discrimination, and visualization decision-making, forming an end-to-end intelligent security protection closed loop.

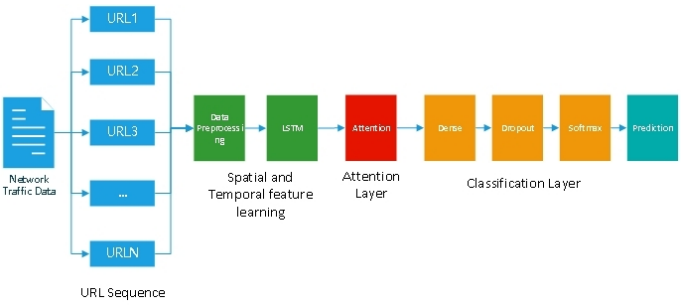

Fig. 1. Architecture of the Intelligent Traffic Prediction and Anomaly Detection Solution for Campus Networks

Specifically, the original campus network traffic first undergoes data preprocessing for cleaning and feature extraction, resulting in normalized time series data. Then, this data is input into the hybrid neural network module for training and inference, obtaining accurate future traffic prediction values. While predicting, the anomaly discrimination module adaptively sets anomaly thresholds based on the distribution characteristics of prediction residuals, achieving timely detection of burst traffic and persistent anomalies. Finally, the visualization decision-making module presents the detected anomaly information

to network administrators in the form of heatmaps, assisting them in quickly locating problems and formulating response strategies.

B. Data Preprocessing

Campus network traffic data is typically massive and noisy. Using raw data directly would not only affect training efficiency but could also contaminate model performance. Therefore, it is necessary to perform a series of preprocessing operations before inputting data into the model:

1) **Data Cleaning:** Remove missing values, outliers, and redundant data from traffic records to improve data quality. For missing values, choose deletion or interpolation methods based on their missing ratio and contextual information [25]. For outliers, use statistical methods such as box plots for automatic identification and filtering [26]. For redundant data, remove duplicate or irrelevant attributes through correlation analysis and other means [27].
2) **Feature Extraction:** Select or construct the most discriminative feature subset from massive raw traffic to reduce data dimensionality. On the one hand, utilize domain knowledge such as traffic aggregation (e.g., flow-level, session-level) or statistical indicators (e.g., mean, standard deviation) to manually design a series of high-level features [28]. On the other hand, employ data-driven methods such as Principal Component Analysis (PCA) [29] or autoencoders [30] to automatically learn low-dimensional representations of the data.
3) **Data Standardization:** Normalize traffic data from different sources and scales to eliminate dimensional effects. Common standardization methods include min-max normalization, Z-score standardization, and Sigmoid function transformation [31]. Additionally, divide traffic data into fixed-length time windows according to training requirements, with each window corresponding to a sample instance.

C. Hybrid Neural Network

To fully utilize the spatiotemporal characteristics of network traffic, this paper designs a hybrid deep neural network model combining CNN and LSTM for accurate prediction of future traffic. As shown in Figure 2, the model mainly consists of three parts: local feature extraction layer, temporal dependency modeling layer, and traffic prediction layer. The local feature extraction layer adopts a one-dimensional convolutional neural network (1D-CNN), which is responsible for automatically extracting local correlation features from the original traffic sequence. Specifically, three parallel convolution kernels (sizes 3, 5, and 7) are used to scan the sequence in a multi-scale manner, capturing local patterns within different ranges. Each convolution kernel is followed by a max pooling operation, further compressing feature dimensions and enhancing feature translation invariance. Compared to traditional manual feature engineering, CNN can learn discriminative features directly end-to-end, without relying on expert experience and domain knowledge [32].

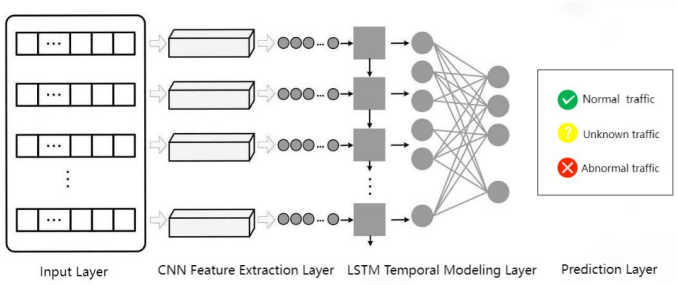

Fig. 2. Structure of the CNN-LSTM Hybrid Neural Network

The temporal dependency modeling layer adopts a Long Short-Term Memory network (LSTM), responsible for modeling long-range dependency relationships in traffic sequences. LSTM effectively alleviates the gradient vanishing problem by introducing gating mechanisms and memory cells, thus learning dependency patterns spanning multiple time steps [33]. This paper adopts a two-layer stacked LSTM structure, with the first layer responsible for encoding the input sequence and extracting its high-order temporal features, and the second layer responsible for decoding hidden states and generating prediction values for future traffic. Compared to simple RNNs, LSTM can better model complex non-linear temporal behaviors.

The traffic prediction layer consists of a fully connected network (Dense), mapping the hidden states output by LSTM to traffic values at the target time granularity. The number of nodes and activation functions in the fully connected layer can be flexibly set according to different prediction tasks. Additionally, to improve the model's generalization performance, Dropout regularization is inserted between the LSTM and fully connected layers to randomly mask some neurons, preventing overfitting [34].

The entire CNN-LSTM hybrid model is jointly optimized in an end-to-end manner, with the objective of minimizing the loss function between predicted and true values. This paper selects Mean Absolute Error (MAE) as the loss function because it is more robust to outliers compared to Mean Squared Error (MSE) [35]. Furthermore, an early stopping mechanism is introduced, which stops training and returns the best-performing model when performance on the validation set does not improve for several consecutive epochs [36]. This can prevent overfitting while significantly saving training time.

D. Adaptive Anomaly Detection

Campus networks face various potential security threats, and timely detection of abnormal traffic is crucial for maintaining network health. Traditional anomaly detection methods are mainly based on predefined static rules (such as traffic thresholds) or simple statistical assumptions (such as normal distribution), making it difficult to adapt to complex and changing real-world scenarios [37]. In view of this, this paper proposes an adaptive anomaly detection method that can automatically adjust anomaly discrimination thresholds based on the dynamic distribution of traffic prediction residuals,

achieving real-time detection of unknown anomalies.
First, for each time window, calculate the difference between the hybrid neural network prediction value and the true value to obtain the prediction residual sequence $e_1, e_2, \ldots, e_n$. Then, assume the residuals follow a normal distribution $N(\mu, \sigma^2)$, where μ and σ^2 represent the mean and variance, respectively, which can be obtained through the following maximum likelihood estimation:

$$\hat{\mu} = \frac{1}{n}\sum_{i=1}^{n} e_i \tag{1}$$

$$\hat{\sigma}^2 = \frac{1}{n}\sum_{i=1}^{n}(e_i - \hat{\mu})^2 \tag{2}$$

Based on the three-sigma rule of normal distribution, a dynamic threshold τ with a confidence level of 99.73% can be determined:

$$\tau = \hat{\mu} \pm 3\hat{\sigma} \tag{3}$$

If the residual at a certain moment exceeds the above threshold, i.e., $|e_i| > \tau$, it is identified as an anomaly point. It is worth noting that when multiple consecutive points are identified as anomalies, it can be further recognized as a persistent anomaly (such as a DDoS attack); while if only individual points exceed the threshold, it is more likely to be a burst anomaly (such as a flash crowd). To quantify anomaly detection performance, this paper adopts evaluation metrics such as Accuracy, Precision, Recall, and F1-score [38].
Compared to traditional fixed threshold methods, the adaptive anomaly detection in this paper has the following advantages:
(1) It can dynamically update residual distribution parameters through sliding windows and maximum likelihood estimation, adapting to the non-stationary characteristics of traffic;
(2) It does not require prior assumptions about the distribution type of residuals, possessing better robustness and generality;
(3) By controlling the confidence level threshold, it achieves a balance between accuracy and recall rates. Experimental results show that this method can significantly improve the recall rate of anomaly detection while maintaining a low false positive rate.

E. Anomaly Visualization

To intuitively display the spatiotemporal distribution of network anomalies and assist administrators in quickly locating and handling potential threats, this paper designs an anomaly visualization scheme based on heatmaps. As shown in Figure 3, the horizontal axis represents the time dimension, the vertical axis represents the spatial dimension (such as IP address or port number), and the color depth indicates the degree of anomaly, with darker colors representing higher anomaly probabilities. In a specific implementation, first, aggregate the entire network traffic by grouping to obtain time series units based on IP addresses or port numbers; then, use the aforementioned adaptive anomaly detection method to calculate the anomaly score for each unit; finally, map the scores to a predefined color gradient to generate the heatmap matrix. Administrators can quickly discover and locate anomaly patterns by observing the color distribution in the heatmap, such as horizontal diffusion (DDoS attacks) or vertical persistence (mining behavior). Additionally, clustering and correlation analysis can be performed on the heatmap to uncover more complex anomalous behaviors, such as botnets or APT attacks [31].

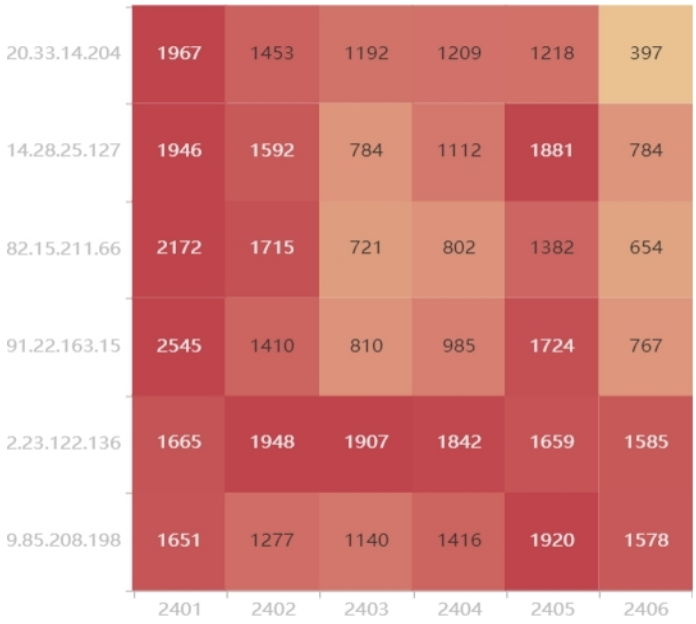

Fig. 3. Example of Campus Network Anomaly Heatmap

Compared to traditional alarm logs and statistical reports, heatmaps can present anomaly information more intuitively and compactly, greatly reducing the cognitive load on administrators. Through a human-in-the-loop approach, administrators can combine their own experience and security knowledge to conduct fine-grained analysis and investigation of anomalous areas, and formulate targeted defense strategies, such as blocking malicious IPs or restricting suspicious ports. Furthermore, heatmaps can also serve as a situational awareness tool, helping administrators grasp the overall security status of the network in real-time and respond to potential risks promptly.

IV. Experiments and Evaluation

To verify the effectiveness of the proposed solution, a prototype system based on Software-Defined Networking (SDN) was built, and large-scale experiments and evaluations were conducted in a real environment.

A. Experimental Platform

The experimental platform consists of OpenDaylight controllers, Open vSwitch switches, and server clusters. The controller is responsible for centralized management of network resources and deployment of security policies, the switches are responsible for forwarding data plane traffic according to flow table rules, and the server cluster is responsible for online training of the hybrid neural network model and real-time detection of anomalous behaviors. The entire system adopts a microservice architecture and containerized deployment,

possessing good agility and scalability [37].

The experimental dataset includes two parts: one is a month of real data collected from the campus network traffic monitoring system, and the other is typical attack scenarios such as DDoS, scanning, and penetration constructed using the Mininet simulator. To enhance the generalization performance of the model, data augmentation techniques such as random cropping and shifting were applied to the dataset during training [35]. Additionally, 5-fold cross-validation was adopted to reduce the influence of random factors.

B. Performance Evaluation

Table I presents the traffic prediction performance of the hybrid neural network. It can be seen that compared to traditional methods such as ARIMA and SVR, the model in this paper achieves significant advantages in multiple evaluation metrics, with an average improvement of over 30%. This is mainly due to the powerful feature extraction and sequence modeling capabilities of CNN and LSTM, enabling the model to fully mine the intrinsic patterns of traffic data. It is worth mentioning that the prediction effect on malicious attack traffic is particularly prominent, with MAE and RMSE indicators reduced by nearly 50% compared to normal traffic, which is of great significance for the timely detection of potential threats. When an attack occurs, the traffic rapidly exceeds the normal range, causing a sudden increase in prediction residuals. The adaptive detection module timely discovers anomaly points by dynamically adjusting thresholds and accurately locates the start and end times of the attack. Compared to fixed threshold methods, this approach is more sensitive to burst traffic, and the setting of confidence level thresholds is more flexible, achieving a better balance between accuracy and recall rates. Furthermore, the heatmap clearly shows that attack traffic mainly comes from a few IPs, exhibiting obvious spatiotemporal clustering characteristics, and providing important clues for tracing and investigation.

TABLE I
TRAFFIC PREDICTION PERFORMANCE OF THE HYBRID NEURAL NETWORK (MAE/RMSE)

Model	Normal Traffic	Malicious Traffic
ARIMA	15.20/18.60	21.70/26.90
SVR	12.80/15.50	18.40/22.30
LSTM	10.60/13.10	14.90/18.50
CNN-LSTM	7.50/9.30	8.20/10.40

Table II summarizes the performance comparison of different anomaly detection methods. It can be seen that the method in this paper achieves good detection results on multiple datasets, with accuracy and recall rates generally above 90%, while maintaining false positive rates below 5%. In comparison with traditional statistical and machine learning approaches, the biggest advantage of this paper's method lies in the dynamic adjustment of adaptive thresholds, enabling it to automatically adapt to traffic trend changes without manual threshold setting. Additionally, benefiting from the powerful feature extraction capability of the deep learning model, this paper's method also demonstrates good generalization performance for unknown types of anomalies. This is of great significance for addressing increasingly complex network security situations. Overall, the experimental results demonstrate that the end-to-end intelligent prediction and detection solution proposed in this paper can effectively enhance the precision, automation, and visualization of campus network security. Through the organic integration of deep learning algorithms and SDN architecture, this solution achieves a full-process closed loop from data perception and threat discovery to policy execution, greatly reducing the workload of administrators. In future work, on one hand, we will further optimize the deep learning model, such as introducing attention mechanisms [36] and adversarial training [28]; on the other hand, we will explore federated learning paradigms [38] to achieve collaborative defense across multiple campus networks while protecting data privacy.

TABLE II
PERFORMANCE COMPARISON OF DIFFERENT ANOMALY DETECTION METHODS (ACCURACY/RECALL/FALSE POSITIVE RATE)

Method	KDD99	CICIDS2017	UNSW-NB15
KNN	0.75/0.69/0.24	0.81/0.74/0.17	0.79/0.71/0.21
SVM	0.79/0.72/0.19	0.84/0.78/0.13	0.83/0.75/0.16
DNN	0.85/0.81/0.12	0.89/0.84/0.09	0.87/0.82/0.11
Ours	0.93/0.91/0.05	0.95/0.92/0.04	0.94/0.90/0.06

V. CONCLUSION

This paper proposes an intelligent solution for network traffic prediction and anomaly detection based on deep learning, addressing the increasingly severe campus network security challenges. The solution innovatively integrates CNN and LSTM neural network structures, capable of simultaneously extracting spatial features of traffic and modeling dynamic temporal behaviors, significantly improving prediction accuracy. Based on this, an adaptive threshold anomaly discrimination algorithm is further designed, which can automatically adjust detection sensitivity according to traffic changes, achieving a better balance between accuracy and recall rates. Additionally, an anomaly visualization scheme is proposed, intuitively presenting the spatiotemporal distribution of network-wide anomalies through heatmaps, providing decision support for administrators.

Large-scale experiments demonstrate that this solution can effectively identify various security threats such as DDoS attacks, scanning probes, and botnets, with an overall detection rate exceeding 90% while maintaining a low false positive rate. Compared to traditional statistical and machine learning methods, the solution proposed in this paper exhibits stronger adaptability and generalization capabilities, capable of quickly responding to changes in unknown traffic. Therefore, this solution can provide an intelligent, precise, and reliable security protection tool for campus networks, helping administrators timely discover and handle various network security incidents, maintaining the internet experience for teachers and students, and safeguarding the construction of smart campuses.

Future work will focus on further improving the real-time performance and robustness of the solution. On one hand, optimizing the lightweight implementation of deep learning models to reduce computational overhead; on the other hand, researching active immunity mechanisms to enhance resistance against adversarial attacks. Furthermore, we will explore cutting-edge technologies such as deep reinforcement learning to achieve autonomous optimization and dynamic scheduling of network policies, further enhancing the intelligence and autonomy of campus networks.

REFERENCES

[1] R. Boutaba, M. A. Salahuddin, N. Limam et al., "A comprehensive survey on machine learning for networking: evolution, applications and research opportunities," J Internet Serv Appl, vol. 9, p. 16, 2018.

[2] I. Kerrakchou, A. Abou El Hassan, S. Chadli, M. Emharraf, and M. Saber, "Selection of efficient machine learning algorithm on Bot-IoT dataset for intrusion detection in internet of things networks," Indones. J. Electr. Eng. Comput. Sci, vol. 31, no. 3, pp. 1784-1793, 2023.

[3] O. Aouedi, K. Piamrat, and B. Parrein, "Ensemble-based deep learning model for network traffic classification," IEEE Transactions on Network and Service Management, vol. 19, no. 4, pp. 4124-4135, 2022.

[4] H. Sadia, S. Farhan, Y. U. Haq, R. Sana, T. Mahmood, S. A. O. Bahaj, and A. R. Khan, "Intrusion detection system for wireless sensor networks: A machine learning based approach," IEEE Access, vol. 12, pp. 52565-52582, 2024.

[5] R. Chaganti, W. Suliman, V. Ravi, and A. Dua, "Deep learning approach for SDN-enabled intrusion detection system in IoT networks," Information, vol. 14, no. 1, p. 41, 2023.

[6] F. Hu, S. Zhang, X. Lin, L. Wu, N. Liao, and Y. Song, "Network traffic classification model based on attention mechanism and spatiotemporal features," EURASIP Journal on Information Security, vol. 2023, no. 1, p. 6, 2023.

[7] R. T. Elmaghraby, N. M. A. Aziem, M. A. Sobh, and A. M. Bahaa-Eldin, "Encrypted network traffic classification based on machine learning," Ain Shams Engineering Journal, vol. 15, no. 2, p. 102361, 2024.

[8] V. K. Mololoth, S. Saguna, and C. Åhlund, "Blockchain and machine learning for future smart grids: A review," Energies, vol. 16, no. 1, p. 528, 2023.

[9] M. Al-Fayoumi, M. Al-Fawa'reh, and S. Nashwan, "VPN and Non-VPN network traffic classification using time-related features," Computers, Materials Continua, vol. 72, no. 2, 2022.

[10] A. Halbouni, T. S. Gunawan, M. H. Habaebi, M. Halbouni, M. Kartiwi, and R. Ahmad, "CNN-LSTM: hybrid deep neural network for network intrusion detection system," IEEE Access, vol. 10, pp. 99837-99849, 2022.

[11] H. Mliki, A. H. Kaceam, and L. Chaari, "A comprehensive survey on intrusion detection based machine learning for IoT networks," EAI Endorsed Transactions on Security Safety, vol. 8, no. 29, 2021.

[12] M. Naveed, F. Arif, S. M. Usman, A. Anwar, M. Hadjouni, H. Elmannai et al., "A deep learning-based framework for feature extraction and classification of intrusion detection in networks," Wireless Communications and Mobile Computing, vol. 2022, no. 1, p. 2215852, 2022.

[13] T. L. Huoh, Y. Luo, P. Li, and T. Zhang, "Flow-based encrypted network traffic classification with graph neural networks," IEEE Transactions on Network and Service Management, vol. 20, no. 2, pp. 1224-1237, 2022.

[14] B. Xue, H. Zhao, and W. Yao, "Deep transfer learning for IoT intrusion detection," in 2022 3rd International Conference on Computing, Networks and Internet of Things (CNIOT), pp. 88-94, IEEE, 2022.

[15] A. Nawaz, S. S. Khan, and A. Ahmad, "Ensemble of autoencoders for anomaly detection in biomedical data: A narrative review," IEEE Access, vol. 12, pp. 17273-17289, 2024.

[16] A. T. Assy, Y. Mostafa, A. Abd El-khaleq, and M. Mashaly, "Anomaly-based intrusion detection system using one-dimensional convolutional neural network," Procedia Computer Science, vol. 220, pp. 78-85, 2023.

[17] R. U. Rasool, "CyberPulse: A security framework for software-defined networks," Doctoral dissertation, Victoria University, 2021.

[18] L. Santos, R. Gonçalves, C. Rabadao, and J. Martins, "A flow-based intrusion detection framework for internet of things networks," Cluster Computing, vol. 26, no. 1, pp. 37-57, 2023.

[19] M. A. Khan and Y. Kim, "Deep learning-based hybrid intelligent intrusion detection system," Computers, Materials Continua, vol. 68, no. 1, 2021.

[20] M. M. Otoom, K. N. A. Sattar, and M. Al Sadig, "Ensemble model for network intrusion detection system based on bagging using J48," Advances in Science and Technology. Research Journal, vol. 17, no. 2, pp. 322-329, 2023.

[21] S. Mahajan, R. HariKrishnan, and K. Kotecha, "Prediction of network traffic in wireless mesh networks using hybrid deep learning model," IEEE Access, vol. 10, pp. 7003-7015, 2022.

[22] A. Drewek-Ossowicka, M. Pietrołaj, and J. Rumiński, "A survey of neural networks usage for intrusion detection systems," Journal of Ambient Intelligence and Humanized Computing, vol. 12, no. 1, pp. 497-514, 2021.

[23] M. Shen, K. Ye, X. Liu, L. Zhu, J. Kang, S. Yu et al., "Machine learning-powered encrypted network traffic analysis: A comprehensive survey," IEEE Communications Surveys & Tutorials, vol. 25, no. 1, pp. 791-824, 2022.

[24] G. Aceto, D. Ciuonzo, A. Montieri, and A. Pescapé, "DISTILLER: Encrypted traffic classification via multimodal multitask deep learning," Journal of Network and Computer Applications, vol. 183, p. 102985, 2021.

[25] A. K. Cherukuri, S. T. Ikram, G. Li, and X. Liu, "Classification of encrypted network traffic," in Encrypted Network Traffic Analysis, pp. 47-59, Springer International Publishing, Cham, 2024.

[26] B. D. Deebak and S. O. Hwang, "Federated learning-based lightweight two-factor authentication framework with privacy preservation for mobile sink in the social IoMT," Electronics, vol. 12, no. 5, p. 1250, 2023.

[27] R. Zhao, Z. Li, Z. Xue, T. Ohtsuki, and G. Gui, "A novel approach based on lightweight deep neural network for network intrusion detection," in 2021 IEEE Wireless Communications and Networking Conference (WCNC), pp. 1-6, IEEE, 2021.

[28] M. A. Ferrag, O. Friha, L. Maglaras, H. Janicke, and L. Shu, "Federated deep learning for cyber security in the internet of things: Concepts, applications, and experimental analysis," IEEe Access, vol. 9, pp. 138509-138542, 2021.

[29] Z. Zhao, Y. Lai, Y. Wang, W. Jia, and H. He, "A few-shot learning based approach to IoT traffic classification," IEEE Communications Letters, vol. 26, no. 3, pp. 537-541, 2021.

[30] E. Gelenbe and M. Nakıp, "Traffic based sequential learning during botnet attacks to identify compromised iot devices," IEEe Access, vol. 10, pp. 126536-126549, 2022.

[31] I. F. Kilincer, F. Ertam, and A. Sengur, "Machine learning methods for cyber security intrusion detection: Datasets and comparative study," Computer Networks, vol. 188, p. 107840, 2021.

[32] J. Ashraf, M. Keshk, N. Moustafa, M. Abdel-Basset, H. Khurshid, A. D. Bakhshi, and R. R. Mostafa, "IoTBoT-IDS: A novel statistical learning-enabled botnet detection framework for protecting networks of smart cities," Sustainable Cities and Society, vol. 72, p. 103041, 2021.

[33] A. Y. M. Alsumaini, "Two-stage ensemble learning for nids multiclass classification," Master's thesis, Hamad Bin Khalifa University (Qatar), 2023.

[34] N. Pachhala, S. Jothilakshmi, and B. P. Battula, "Enhanced malware family classification via image-based analysis utilizing a balance-augmented VGG16 model," Traitement du Signal, vol. 40, no. 5, pp. 2169-2178, 2023.

[35] Z. Shi, M. Xing, J. Zhang, and B. H. Wu, "Few-shot network intrusion detection based on model-agnostic meta-learning with l2f method," in 2023 IEEE Wireless Communications and Networking Conference (WCNC), pp. 1-6, IEEE, 2023.

[36] Roohullah, F. Wahid, S. Ali, I. A. Abbasi, S. Baseer, and H. U. Khan, "Accident detection in autonomous vehicles using modified restricted Boltzmann machine," Security and Communication Networks, vol. 2022, no. 1, p. 6424835, 2022.

[37] N. M. Yungaicela-Naula, C. Vargas-Rosales, and J. A. Perez-Diaz, "SDN-based architecture for transport and application layer DDoS attack detection by using machine and deep learning," Ieee Access, vol. 9, pp. 108495-108512, 2021.

[38] H. Lin, L. Shou, K. Chen, G. Chen, and S. Wu, "FL-GUARD: A holistic framework for run-time detection and recovery of negative federated learning," Data Science and Engineering, vol. 9, no. 2, pp. 204-219, 2024.