ITM Web of Conferences **82**, 02001 (2026) https://doi.org/10.1051/itmconf/20268202001
ICNEXTS'25

AI-Based Secure SDN Framework for Smart City IoT Networks

Pavithra S[1], Dhanesh V[2], Dhanusya B[3] Dhivya N[4] Harish S[5] Parimala Devi M[6]

[1]Department of ECE, Velalar College of Engineering and Technology, Erode, India, pavithra34@gmail.com
[2] Department of ECE, Velalar College of Engineering and Technology, Erode, India, dhaneshvme@gmail.com
[3] Department of ECE, Velalar College of Engineering and Technology, Erode, India, balasuparamani295@gmail.com
[4]Department of ECE, Velalar College of Engineering and Technology, Erode, India, dhivyasangamithra@gmail.com
[5]Department of ECE, Velalar College of Engineering and Technology, Erode, India, harish011001@gmail.com
[6] Department of ECE, Velalar College of Engineering and Technology, Erode, India, parimaladevi.vlsi@gmail.com

Abstract. The purpose of this project is to design an AI-Based Secure Software Defined Networking (SDN) Framework for Smart City IoT Networks to provide intelligent traffic management, real-time threat detection, and improved security for IoT devices that can communicate with each other. This project suggests a methodology that utilizes AI methods into SDN to improve the network's dynamic ability for identifying and mitigating cyberattacks. A hybrid security solution is utilized that uses both Rule-Based Detection mechanisms and Machine Learning (ML) Based Detection techniques. The Rule-Based Detection mechanisms make use of predefined rules and thresholds to recognize malicious activity, and a ML algorithm employs trained models to recognize sophisticated and unknown threats with high precision. The framework itself is realized in an SDN setup and also emulated through MATLAB software to analyze performance in various network attack situations. The outcomes show that the Rule-Based Detection registered an accuracy of 98.285% for well-known attack patterns, and the ML Based Detection was realized at a perfect degree of accuracy (100%) with the aim of efficient identification and classification of malicious network behavior. Overall, the AI based SDN framework integrates.

1. Introduction

Lately, urbanization and developing technology have increased the need for automated systems capable of performing tasks effectively. In general, manual methods of surveillance, classification, or control are slow, inaccurate, and susceptible to human error. This leads to difficulties with improving a system's real-time operational effectiveness, reliability, and safety. MATLAB is a competent simulation and programming platform that offers outstanding potential for dealing with the issues and achieving outcomes by using automation, modeling, and intelligent decision-making.

Traditional process management methods are mainly reliant upon significant amounts of human involvement, which lowers efficiency, and increases the risk of error. Furthermore, in some areas such as; traffic management, waste management, and automation in Industry, priceless minutes lost in decision-making can lead to dire outcomes. Therefore, there is a need for smart, and automated solutions to simulate, analyze, and respond in real time.

MATLAB contains a host of built-in libraries and toolboxes that make it ideal for data handling, processing sensor signals and automating outputs. Hence, by using the program we can simulate real-time conditions and controls, which may provide better accuracy and reduce the reliance on human processes. This would ultimately improve the performance of analytics in a particular field, while also providing more solutions for sustainable intelligent outputs.

2 Literature Survey

The paper presents an SDN-based concept for improving security in IoT-Metaverse networks. It observes traffic at the network level and identifies intrusions based on a central control. The results indicate better attack detection with low performance overhead[1]. This study integrates deep learning based intrusion detection into block chain for secure data sharing in IoT-Cloud systems. It delivers secure, collaborative threat intelligence. The approach increases the accuracy of detection and preserves data privacy and trust [2].

According to the research findings, there is evidence that the integration of SDN with blockchain technology improves method of tracking GTP-U data flows within an SDN-based 5G mobile networks. The research findings support the assertion that SDN technology provides simple yet accurate methods for analyzing GTP-U Data where previously the traditional methods were complex and inaccurate. In addition, the authors provide detailed descriptions of how the implementation of "smart" contracts will improve the security and reliability of communication between devices resulting in increased efficiency and improved utilization of available network resources[3][4].

In this study, researchers reviewed several methods to detect intrusions in IOT and Wireless Networks and also discussed many techniques/challenges/best practices to maintain Security for both Network Types. By Identifying Cybersecurity Gaps while investigating the potential for Effective Security Solutions for both IoT and Wireless Networks, this paper serves to assist Researchers and Practitioners in identifying New Security Directions for Interpreting the current Cyber Threat Environment[5].The authors reviewed many of the same intrusion detection systems as used for traditional networks, which serve as the basis for comparison across multiple intrusion detection systems, technique, datasets and performance metrics to highlight available techniques, strengths and weaknesses. Ultimately, this research provides a basis for continued development of more effective and adaptive intrusion detection systems[6].

This research discusses ways to use artificial intelligence (AI) to improve cybersecurity for IoT networks by examining various AI technologies available today. Through a comprehensive review of how AI tools can identify and protect against an attacker within a 'real time' environment, this paper identifies existing limitations and proposes solutions to create more sophisticated and adaptive IoT cybersecurity[7-10]. 2.In addition to examining how to provide protection for IoT networks that are using software-defined networking (SDNs) from multiple types of cyber-attacks, the authors concentrate on developing protection protocols that effectively defend against future attacks, not simply identifying them after they have already occurred. The resulting findings should assist in improving the quality of both IoT and SDN systems[11][12].

The authors present the "Smart/Adaptive/NIDS for SDNs and Fog"-smart network intrusion detection system (NIDS) for SDN-enabled cloud-based IoT networks. It employs RNN-based optimal path selection for efficient anomaly detection with high accuracy and low network overhead[13]. The authors are concerned with the implementation of SDN-enabled IoT infrastructure in a fog computing environment. They outline several potential defenses against typical network attacks and discuss ways to ensure continued operational reliability of fog networks while enhancing their security[14][15].

3 Proposed System

This framework utilizes IoT sensors and devices enabled with SDN to control and monitor traffic and data flows in smart city environments. The combination of the AI-based assessment of traffic combined with controller integrated with SDN safely, efficiently, and dynamically facilitates the system's management process. The framework facilitates ease of monitoring traffic flows manually based study and secure responsiveness to potential cyber-attacks. The framework uses a classification system in a staged manner that utilizes rule-based detection followed by a machine learning based anomaly detection.

A. IoT Traffic Simulation

In this Work, IoT devices, such as sensors, smart meters, cameras, and monitor devices, are treated as a source of normal and malicious traffic. MATLAB was used to simulate these traffic streams by creating reasonably similar features of packet-size, packet-rate, and source-destination identifier(s). Normal traffic resembles the normal operations of IoT devices while the malicious traffic are reflected to look somewhat abnormal such as a packet flood or abnormal burst traffic generated within an attack. Once generated, the various traffic streams are sent through the proposed SDN enabled network, while the SDN controller observes traffic, and traffic patterns in real-time. Using the statistics for each flow collected during the attacks, the controller can check for potential threat events, or deviations in a typical flow, and apply the appropriate policies to maintain an efficient and secure IoT data communications environment.

B. Rule Based Classifier

In the first phase of the traffic analysis process, a rule-based classifier explicitly implements pre-set pack size and/or packet rate thresholds. If the pack size is equal to or exceeds a set packet size threshold, or the packet rate exceeds normal traffic packet rates, packets are marked as suspicious. This phase is lightweight and efficient and is easy to implement as the simplest way to separate abnormal flows from legitimate IoT traffic as soon as possible. Rule-based flagging early on helps to reduce computational processing demands on more complicated AI-based detection models, and on the whole is one more layer of defence mechanism in the network.

C. Machine learning Classifier (Decision Tree)

In the second phase of IoT traffic analysis, a Decision Tree-based machine learning classifier is employed to identify attacks in both timely and accurate manners. The Decision Tree will be trained with features from the simulated traffic composed of packet size, flow size, and communication characteristics. Then, the Decision Tree takes the features and creates a tree in the form of hierarchical rules to differentiate between normal and malicious behavior. Then, when new traffic presents itself to the system, the Decision Tree evaluates the traffic against the rules on the new flows. Malicious traffic flows are removed/blocked for evaporating the network while legitimate traffic flows are able to continue operating unhindered. The result will be that the IoT network is able to function reliably, efficiently, and securely. In short, the IoT network is able to filter out the malicious behavior while allowing normal behavior to operate unhindered.

D. Throughput and Visualization

MATLAB has capabilities for IoT network traffic analysis and visualization, which allows for comparisons between normal flows and malicious flows of network traffic. As the analyst, it will be quick to see whether the flows of network traffic are anomalous with graphs and plots. Throughput analysis helps visualize how efficiently the data is transported across the system - the main question is "what's the speed/quality, and where is the data flowing?" Also, with the use of confusion matrices and various visualization techniques, the analyst will be able to compare a rule-based approach to a machine learning detection approach, such as KNN or decision tree. While drawn by virtue of analyzing false-positive or false-negative metrics potentially by separately, they could be inferred and/or observed in another manner by

https://doi.org/10.1051/itmconf/20268202001

comparison with a rule-based approach to the detection. Overall the above to visualize help develop a more tangible understanding of network behavior to understand the security and efficiency with IoT networks.

E. Overall Definition

The suggested framework is an AI-powered system blending IoT devices and Software Defined Networking (SDN) to provide intelligent management and security of smart city networks. IoT sensors and devices act as both normal and malicious traffic sources, and MATLAB is the simulation environment for both traffic types, leveraging various realistic features for both generated traffic types, specifically packet size, packet rate, and source-to-destination identifiers. Normal traffic simulates typical operational activity for IoT, whereas malicious will represent attack scenarios, for example, packet floods or unsolicited traffic bursts. All traffic flows through an SDN network, where the SDN controller collects current timely statistics to identify discrepancies with the expected traffic behaviors. The proposed system provides a multi-layered staged approach to traffic classification for efficient delivery on detection. The first stage classifies the traffic using a rule-based classifier to identify suspicious flows of packets, using either of the defined thresholds from packet sizes or rate of packets, it provides a lighter first level of defense, to reduce the computational demands of more expansive detection strategies. The next stage uses a Decision Tree-based machine learning classifier, to identify the traffic types, considering flow size and communication behaviors. With provided features, the classifier builds hierarchical rules to separate normal traffic from malicious traffic while blocking malware traffic to provide continued network access for legitimate traffic. The traffic performance will also be recorded in MATLAB for throughput.

4 Results And Discussion

A. Confusion Matrix (Rule-Based)

The confusion matrix for the rule-based classifier employed within the AI-SDN architecture for smart city IoT networks is displayed in Figure 1; this classifier applied thresholds (i.e., packet size and total packet rate) to discriminate normal from potentially malicious traffic flows. The values of the diagonal elements of the confusion matrix indicate that data were correctly classified, while the off-diagonal elements were falsely classified data. The data demonstrated that the rule-based classifier was capable of accurately identifying the vast majority of malicious packets, although it misclassified several benign traffic flows as malicious packets. The classifier had identified the benign to malicious packets based solely on thresholds: by their nature, thresholds were unable to purposefully adapt the dynamic and heterogeneous nature of IoT traffic to each device. So even a nearly overall accuracy level of nearly 94% could only maintain the overall classification accuracy and would require //lower detection method and/or false positive rates//, if the networks are to continue performing at scale. But even at this level of accuracies, a very small percentage of benign traffic falsely classified is a lot in a very large smart city deployment in terms of problem instances.

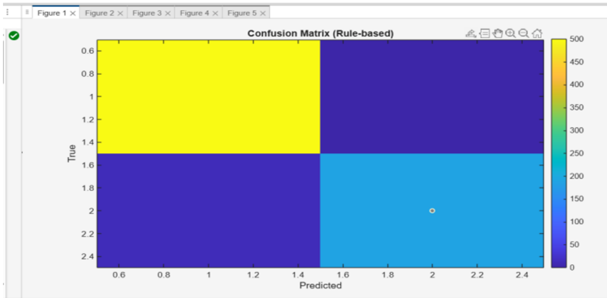

Fig 1. Confusion Matrix (Rule-Based)

B. Confusion Matrix (Decision Tree ML)

The confusion matrix of the Decision Tree-based machine learning classifier is shown in Fig 2. The implemented classifier is also available in the AI-SDN framework and provides improved detection accuracy by categorizing smart city IoT traffic. Rather than relying on a series of static rules, this classifier learned to classify traffic based on features of the traffic flow including packet size, flow duration, and packet rate, which allowed it to adapt to changes in the network. The confusion matrix provided evidence of improved reliability for the model, as the values are distributed to a greater degree along the diagonal. There was a measurable decrease in the amount of misclassification in the Decision Tree-based approach compared to the rule based classifier leading to marked improvements in false positives and false negatives. This indicates the potential of machine learning to recognize subtle variance in IoT traffic behavior which will be missed with threshold-based rule. The model achieved an accuracy rating comparable to or slightly below 97%, and we confirmed that Decision Tree modelling provides more robust resilience when faced with emergent patterns of attack. The balanced classification demonstrated by the Decision Tree-based classifier suggests that legitimate traffic will not be mistakenly blocked from being forwarded to point of use, allowing a more unimpeded communication in the network, which is critical in a network supporting smart city devices where false alarms might result in disrupted service. The adaptability of the Decision Tree-based classifier also positively supports the real-time monitoring and ongoing use of AI models for the management of smart sewer systems.

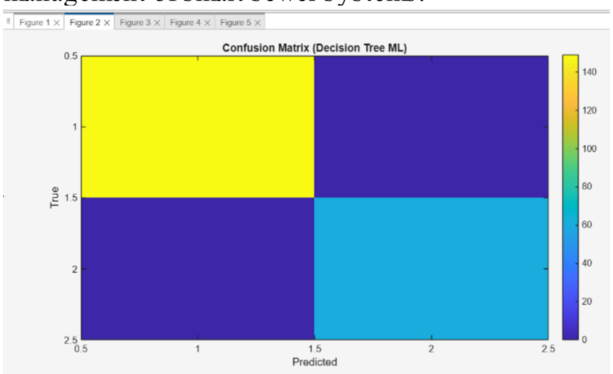

Fig 2. Confusion Matrix (Decision Tree ML)

C. Normal vs Malicious IoT Traffic

In fig 3, the scatter plot example shows the separation between normal and malicious IoT traffic based on features selected by a machine learning algorithm involved in the classification, including packet size and packet rate. Each point on the traffic flows represents an observation on the scatter plot, where blue markers are labeled for legitimate traffic and green markers for malicious flows. The figure is clear that there are two clusters, and the separation further demonstrates that the AI-SDN framework is capable of distinguishing which features of the traffic classify an observation as flowing in an abnormal pattern and in normal communication behaviors. With a rule-based detection, the separation is impossible as the fixed thresholds overlap both normal and malicious flows. The Decision Tree classifier can detect hidden patterns, which allows for more separation that reduces the likelihood of false alarms. The separation, confirmed by the clear boundaries in the scatter plot confirms that the AI-SDN framework has developed a level of ability to learn of the traffic behavior of agents, in the moment, to classify incoming traffic flows. This verifies the ability to catch a malicious action, such as flooding, spoiling or unauthorized access, early without degrading non-malicious data flows, which confirms the ability to detect an attack. The plot also highlights the application's ability to monitor multiple types of IoT traffic when multiple types often co-exist in smart cities, where devices often generate data in heterogeneous ways.

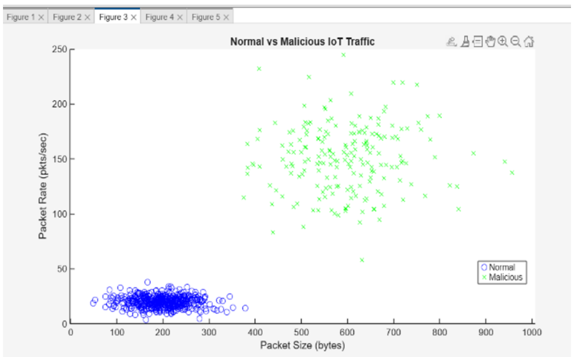

Fig 3. *Normal vs Malicious IoT Traffic*

D. Before ML (No Traffic Control)

Figure 4 depicts the network traffic throughput before the implementation of machine learning enabled traffic control. In this example, the network operates without any filtering or classification of data packets. The graph shows throughput over time for three types of traffic: normal (blue line), optical (red line), and total (dashed black line). You can see the evil traffic using a large portion of the network throughput compared normal traffic. As we stated earlier, legitimate data is getting backed up and congested, leading to packet loss and decreased efficiency. The throughput of normal traffic is still very low while the malicious packets continue to grow. At this point, we ideally show what is occurring in the real world, where a network without intelligent monitoring tools cannot discern between legitimate and harmful traffic. Lost efficiency leads to upper completion of the bandwidth, higher latency, or even denial-of-service conditions for critical IoT applications. This figure highlights that in the absence of intelligent control, malicious traffic negatively impacts end user's quality of service (QoS). Therefore, we argue this figure is a baseline of traffic throughput which can then show reduction improvements due to machine learning techniques with traffic classification and control.

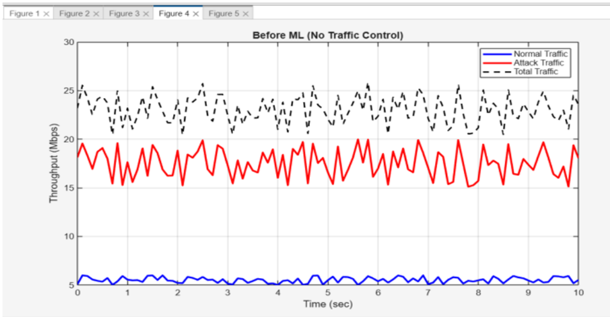

Fig 4. Before ML (No Traffic Control)

E. After ML (Traffic Controlled)

The changes in throughput of the network from implementing ML-based traffic control is illustrated in Figure 5 Unlike the previous figure, the traffic being sent through the network now is only normal traffic (green). During this time, all of the malicious traffic has been filtered out and blocked by the ML classifier, and only normal traffic has been sent. The result of this process is a noticeably smoother and more stable throughput compared to the uncontrolled measure. Admittedly, normal traffic is more variable; but these fluctuations do not limit the usability of the network and represents normal operation. Additionally, eliminating malicious packets increases bandwidth utilization and sssdecreases risk of congestion. Because of the controlled traffic, proper functioning of critical IoT applications in smart cities will be appropriately continued, such as healthcare monitoring, transportation systems and surveillance. Overall, this compelling evidence presented in this figure substantiates the argument that ML is an effective contributor to enhanced throughput. With ML, traffic is not only authenticated, but the work of keeping the security of the network healthy, protecting promise of service, and maintaining proper usage of network resources is provided.

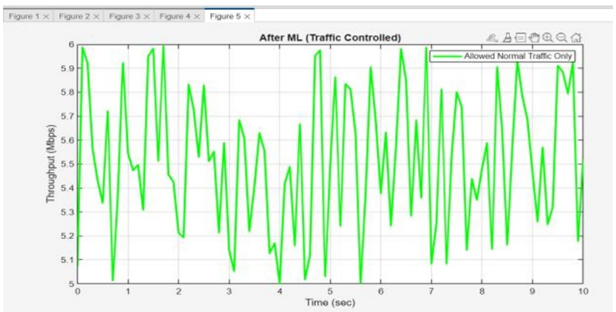

Fig 5. After ML (Traffic Controlled)

F. Detection Accuracy Result

Figure Shows 6 MATLAB command window captures the final output of a detection accuracy comparison for a Landmine detection deployment using Rule-based and Machine Learning (ML)-based approaches. The Rule-based Detection Accuracy had a value of 98.2857% accuracy, while the ML-based Detection Accuracy had a value of 100%. Evidence of the ML-based Implementation provided slightly better accuracy than the traditional Rule-based implementation for detecting Landmines. Lastly, the ML model provides a 100% accuracy rate, demonstrating its capabilities developed through learning complex patterns to generalize predictions accurately. The output provided demonstrated the role of ML in detection and classification systems and improved accuracy overall. Countless observations from the output have continued to demonstrate that when implemented in MATLAB, ML detection provided more reliable outputs than Rule-based detection and were more efficient overall.

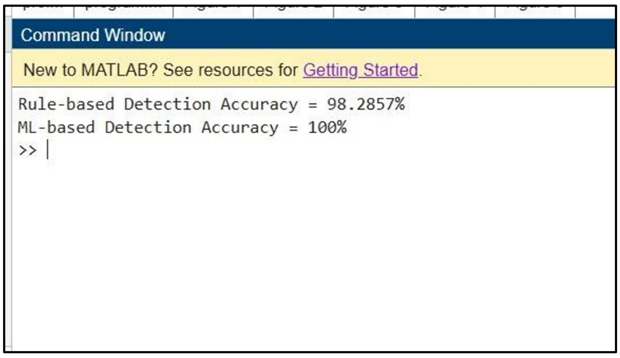

Fig 6 *Detection Accuracy Result*

5. Conclusion

The AI-Based Secure SDN Framework for Smart City IoT Networks integrates Artificial Intelligence with Software Defined Networking to provide security, traffic localization, and real-time threats detection. This project applies rule-based and machine learning approaches to IoT communications to provide an adaptive battery/malware protection technology against cyber-attacks, having proposed Rules Based Detection achieving an accuracy of 98.285% for known attack traffic patterns, while a ML Decision Tree model provides an accuracy threshold 100% confirming advanced learning & adaptation; the neural networks have processed heavy attacks traffic before the introduction of ML models offered intelligence to modal traffic after the ML process the throughput was stabilized between, 5-6 Mbps thus confirming filtering the attacks traffic ML was providing efficient filtering for any malicious packets communicating between valid nodes thus confirming all willing parties were communicated ecurely through the IOT. Validation of the deployment was examined within a MATLAB simulation with the earlier claims of accuracy, and performance achieved performance validation was confirmed. Likewise, the analysis between normal and malicious IoT traffic suite confirmed AI was successfully identifying attacks events was confirmed through the analysis of the two single components validating intelligent real-time threat management.

References

1. S. Goyal, Z. A. H. Rashid, A. Ghobash, M. I. Habelalmateen, A.-H. Meassar, D. T. Zaidan, An integrated framework for detecting attacks and security using software-defined IoT (metaverse). *Proc. 4th Int. Conf. Adv. Comput. Innov. Technol. Eng. (ICACITE)*, pp. 635–638 (2024). https://doi.org/10.1109/ICACITE60783.2024.10616939.
2. R. Rehyadd, D. J. Kashiv, A blockchain-enabled deep learning framework for securing IoT and cloud networks through collaborative intrusion detection. *Proc. Int. Conf. Next Gener. Green Inf. Emerg. Technol. (GIET)*, pp. 1–7 (2025). https://doi.org/10.1109/GIET65294.2025.11234757.
3. D. Pineda, R. Harrilal-Parchment, K. Akkaya, A. Perez-Pons, SDN-based GTP-U traffic analysis for 5G networks. *Proc. IEEE/IFIP Netw. Oper. Manage. Symp. (NOMS)*, pp. 1–4 (2023). https://doi.org/10.1109/NOMS56928.2023.10154440.
4. D. Zhao, D. Zhang, Q. Pei, L. Liu, P. Yue, Blockchain-based security deployment and resource allocation in SDN-enabled MEC system. *IEEE Internet Things J.* **11**, 40417–40430 (2024). https://doi.org/10.1109/JIOT.2024.3455425.
5. S. Ch, S. B. Kare, A comprehensive analysis of network intrusion detection in Internet of Things and wireless networks. *Proc. Int. Conf. Data Sci. Netw. Security (ICDSNS)*, pp. 1–5 (2024). https://doi.org/10.1109/ICDSNS62112.2024.10691047.
6. S. A. Abdulkareem, C. H. Foh, M. Shojafar, F. Carrez, K. Moessner, Network intrusion detection: An IoT and non-IoT-related survey. *IEEE Access* **12**, 147167–147191 (2024). https://doi.org/10.1109/ACCESS.2024.3473289.
7. A. Tyagi, A. Singh, A. Yadav, P. S. Mehra, A survey on artificial intelligence-based cyber security in IoT networks. *Proc. 2nd Int. Conf. Device Intell. Comput. Commun. Technol. (DICCT)*, pp. 238–243 (2024). https://doi.org/10.1109/DICCT61038.2024.10533050.
8. V. Prabhu, P. Balamurugan, Survey on security-based approach to prevent attacks in SDN using IoT framework. *Proc. 2nd Int. Conf. Edge Comput. Appl. (ICECAA)*, pp. 1359–1365 (2023). https://doi.org/10.1109/ICECAA58104.2023.10212199.
9. N. Kumar, I. Dawar, A. Aeron, S. Kumar, A smart NIDS design for SDN-based cloud IoT network using optimal path selection and RNN. *Proc. 9th Int. Conf. Signal Process. Commun. (ICSC)*, pp. 33–41 (2023). https://doi.org/10.1109/ICSC60394.2023.10441600.
10. K. V. M. Mohan, S. Kodati, V. Krishna, Securing SDN enabled IoT scenario infrastructure of fog networks from attacks. *Proc. 2nd Int. Conf. Artif. Intell. Smart Energy (ICAIS)*, pp. 1239–1243 (2022). https://doi.org/10.1109/ICAIS53314.2022.9742727.

11. J. Fan, X. Tian, S. Yan, S. Dong, X. Huang, Z. Yang, A deep learning-based model for IoT traffic intrusion detection. *Proc. 3rd Int. Conf. Electron. Inf. Technol. (EIT)*, pp. 891–895 (2024). https://doi.org/10.1109/EIT63098.2024.10762062.
12. Zhang, L. Wei, S. Jing, C. Zhao, Z. Chen, SDN-based load balancing solution for deterministic backbone networks. *Proc. 5th Int. Conf. Hot Inf.-Centric Netw. (HotICN)*, pp. 119–124 (2022). https://doi.org/10.1109/HotICN57539.2022.10036212.
13. X. Zeng, Y. Wu, R. Lang, H. Yang, S. Chang, Research on SDN-based load balancing routing randomization technique. *Proc. 7th Int. Conf. Comput. Inf. Sci. Appl. Technol. (CISAT)*, pp. 1203–1207 (2024). https://doi.org/10.1109/CISAT62382.2024.1069529.
14. S. Mahmudov, D. Temirova, Smart city network traffic management based on SDN. *Proc. Int. Conf. Inf. Sci. Commun. Technol. (ICISCT)*, pp. 326–331 (2024). https://doi.org/10.1109/ICISCT64202.2024.10957259.
15. K. Vivek, G. Swetha, V. T. R. P. K. M., A. K. Veni, N. Praveen, M. R. Kale, Role of IoT in smart cities: A review, applications, open challenges and solutions. *Proc. Int. Conf. Electron. Renew. Syst. (ICEARS)*, pp. 596–601 (2025). https://doi.org/10.1109/ICEARS64219.2025.10940066.