Journal of Wireless Networks and Communication Systems
Vol. 2, Issue. 2, Apr-Jun 2026, pp. 26~36
ISSN: 3107-6432, DOI: 10.32595/jwncs/v2i2.2026.30

A Zero-Trust Software-Defined Networking Architecture for Secure and Trustworthy AIoT Environments

P.S.G. Aruna Sri[1], Dr.D.Saveetha[2]

[1]Professor, Department of Internet of Things, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India.
E-mail: arunasri_2012@kluniversity.in
[2]Assistant Professor, Department of Networking and Communications, SRMIST, Kattankulathur, 603203, Chennai, Tamilnadu, India.
E-mail: saveethd@srmist.edu.in

Article Info

Article History:

Received Apr 09, 2026
Revised May 08, 2026
Accepted Jun 06, 2026

Keywords:

Software Defined Networking,
Internet of Things,
Deep Learning,
Network Security,
Trust Management

ABSTRACT

This paper describes a Zero-Trust Software-Defined Networking (ZT-SDN) architecture, which has been developed to create secure and trustworthy AIoT environments and provide enhanced network performance overall. The innovative architecture proposed in this paper uses the combination of deep learning-based anomaly detection, trust-aware adaptive routing and continuously-verifying mechanisms to manage network traffic securely and in real time. This is achieved through the continuous monitoring of network activity, real-time detection of malicious activity, and the dynamic updating of SDN flow rules based upon trust evaluation. Experimental results prove the effectiveness of the developed model as compared to traditional methods of machine-learning based approaches in that it achieved an accuracy rate in the area of attack detection greater than 12%, for total of 96.8%. Additionally, using this method reduced packet loss by 30%, lowered the amount of delay (network latency) under heavy (high volume) traffic conditions by 21%, and increased throughput by 18%. The combination of Zero Trust enforcement and Trust Aware Routing provides a means of ensuring the security of transmitted data, as well as mitigating adverse effects from compromised nodes. Thus, the developed Zero Trust SDN Framework provides the user with greater levels of security; scalability; and efficiency, and as a result, is very suitable for implementation in smart cities and AIoT applications for industries.

Corresponding Author:

P.S.G. Aruna Sri,
Professor, Department of Internet of Things,
Koneru Lakshmaiah Education Foundation, Vaddeswaram AP, India.
E-mail: arunasri_2012@kluniversity.in

1. INTRODUCTION

As the IoT has evolved at a rapidly growing rate in conjunction with the growth of artificial intelligence (AI) [1], researchers have created a completely new field of study called the artificial

intelligence of things (AIoT). The AIoT allows connected devices to make intelligent decisions, automate processes and perform real-time analytics. AIoT will be critical for applications in areas such as smart cities, industrial automation, remote health monitoring and implementing autonomous transportation systems [3]. There are many issues related to managing large heterogeneous networks of resource-constrained devices and scaling these networks, but the biggest issue is security.

Traditional network architectures tend to have specific traits that restrict their ability to adapt to AIoT networks as they typically have static properties and offer little flexibility in accommodating for the dynamic and decentralized nature of (AIoT) networks [4]. Therefore an alternate means of addressing these issues could be by employing (SDN) software-defined networking as it decouples the control of a switching/routing function from data; however there are security concerns with implementing SDN within connected IoT devices [5]. Examples of these types of challenges include (DDoS) distributed denial-of-service attacks; spoofing attacks; unauthorized access/usage of devices; insider attacks and so on. The act of centralizing control via one or more SDN controllers has also created further opportunities for a centralized point of failure as all end users report their status back to one controller thus making it 'the' prime target of cyber adversaries [6].

The use of perimeter-based recommendations to establish a user trust level on a network has changed with the evolving threats new AIoT ecosystems face, since devices frequently join and leave the network now; therefore, agencies cannot rely upon the initial trust level to determine access. Due to increasing numbers of both internal and external threats to networked systems, the zero trust concept is becoming increasingly popular [7]. As opposed to traditional security models, zero trust assumes that every device is a potential threat until demonstrated otherwise through ongoing authentication, rigid access control and real-time monitoring of every device on the network [8].

At the same time, Artificial Intelligence (AI) has also become increasingly useful for improving network security through the use of advanced Anomaly Detection techniques based on Deep Learning. Compared to traditional Machine Learning techniques which may fail to identify complex, continuous attacks, Deep Learning models are able to identify complex and changing patterns of attack. However, even though Anomaly Detection alone is not able to provide secure communications, intelligent Traffic Management must also be employed in conjunction with Anomaly Detection.

In this work, we present a Zero Trust Software Defined Network (ZT-SDN) architecture specifically designed for the Artificial Intelligence of Things (AIoT) environment to alleviate these challenges. We provide architecture for ZT-SDN, where we fuse Deep Learning based anomaly detection functionality with trust enabled adaptive route selection in order to provide secure communications on the network and to optimize network operations. The anomaly detection module continuously monitors traffic for the detection of possible malicious activity on a real time basis. The trust management module checks the trust level of each node within the network for the purpose of establishing a secure route to communicate with that node.

The findings of this study provide several key contributions to the field:

1. An innovative Zero-Trust Style SDN architecture that was designed for both safety when using AI and IoT.

2. The correlation of machine learning approaches to developing an anomaly detection system and to developing a defence against an attack while it occurs.

3. The development of an adaptive routing method that is trust aware, providing for secure transmission of the data by ensuring that no nodes are compromised while in transit.

4. A recommendation supported by empirical evidence of increased accuracy of incident detection rates, reduced latency, reduced loss of packets and improved throughput as compared to traditional methods.

This paper is divided into four sections; the second section is a study of related research; the third section describes our proposed methodology; the fourth section presents experimental results and discussion, and finally, the last section concludes.

2. LITERATURE REVIEW

[9] Developed the Anomaly Detection and Behavior Identification System (ADBIS) framework utilized machine learning techniques for anomaly detection within an IoT Environment. The ADBIS framework successfully detected malicious activity and improved the security of networks by analyzing patterns of network traffic. Experiments showed a significant increase in performance for detecting anomalies as opposed to traditional security methods; however, ADBIS does not take into account trust-based routing or zero-trust methods for the purpose of providing continual verification of devices.

[10] Developed an intrusion detection system based on the blockchain and deep learning that would be suitable for an SDN-enabled IIoT environment by incorporating resources from two technologies (blockchain and deep learning) into a single model to enhance detection accuracy of attacks and securing communications. Results produced from experiments confirmed increased resistance to cyber attacks but challenges remain due to high computational cost associated with the use of blockchain technology.

Using traffic feature selection techniques, a DDoS attack detection framework for Software-Defined Networks based on machine learning was created by [11]. Their approach demonstrated superior accuracy at detecting DDoS attacks with lower computational complexity than traditional methods. Therefore, intelligent feature selection is a viable option for providing real-time security solutions for SDN (Software-Defined Networks) through the use of machine learning algorithms.

A trust management framework based on graph neural networks has been proposed by [12] for anomaly detection in the Internet of Things (IoT). A model has been created to evaluate the trustworthiness of nodes through the use of graph learning methods and was able to achieve good accuracy for detecting anomaly occurrences within dynamic IoT environments. An important point to note is that this research primarily addressed the limited scope of developing a method for evaluating trust and did not include a method for incorporating centralized software-defined networking (SDN) control into a zero-trust (ZT) security policy.

3. METHODOLOGY

This section lays down the theoretical background and mathematical representation of the new architecture of Zero-Trust Software-Defined Networking for a secure AIoT implementation. The framework comprises the use of the deep learning techniques to be performed on anomaly detection, trust measurement and adaptive routing in accordance with Zero-Trust principles.

3.1 System Model

In the specified AIoT Networks, a Secure AIoT Communication Model is designed utilizing Zero-Trust Principles and Software-Defined Networking. As seen in Figure 1, the Safeguard AIoT Communication Model consists of a variety of elements working together to ensure secure communications.

An IoT device will transmit data to the SDN switch, which will in turn relay that data to the SDN Controller. When the SDN Controller receives data from the IoT Device, it performs a traffic analysis from an attached deep-learning-based anomaly detection module to detect potentially malicious activities. The flow of the data is then analyzed; data traffic is affected by a Trust Management System that assigns Trust Scores to determine the reliability of the IoT devices. Each device is verified by the Zero-Trust principle prior to allowing them to communicate. In addition to the Trust Score assigned to the device, the SDN Controller has updated flow rules to control the data being sent over the network based on the performed flow and Trust Score analyses, such that data is only sent through trusted, secure paths within the network to ensure secure, safe, and efficient communication.

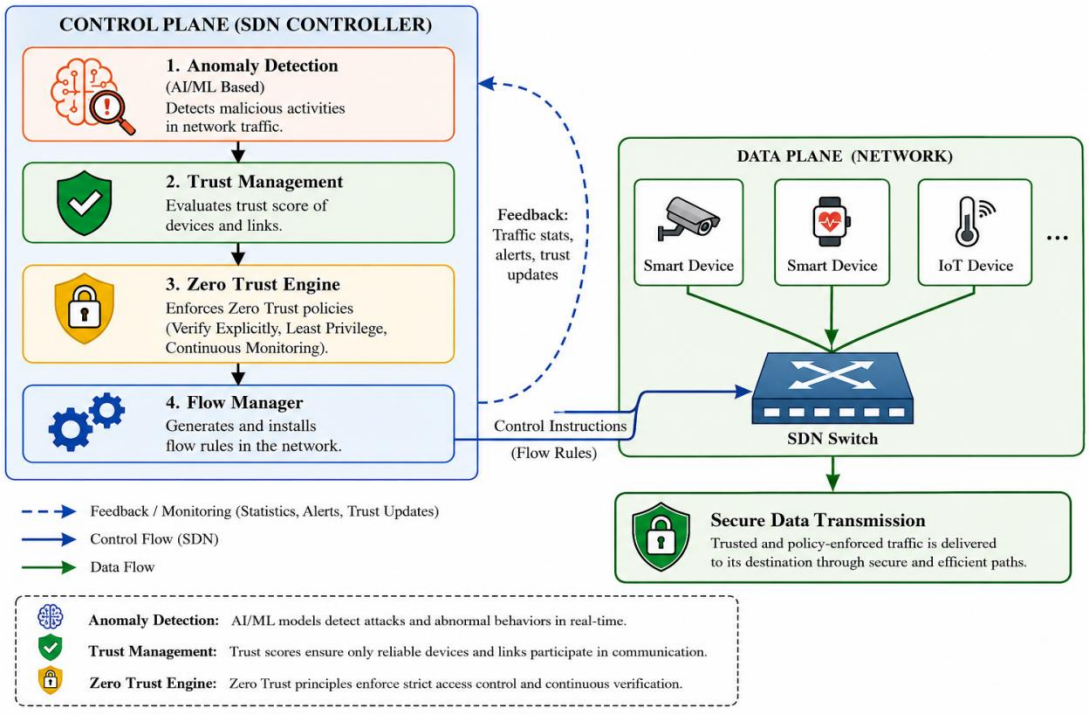

Figure 1. Proposed Zero-Trust SDN Architecture

The architecture of the AI oT network is a dynamically-generated graph, in which all of the IoT devices (nodes) and their means of communication (edges) are represented. In the continuous evolution of IoT environments, the states of all nodes and links are constantly shifting as IoT devices move around and as the status of communication links change due to various factors. For this reason, the SDN controller maintains a single global perspective of the entire AIoT(i.e., All Internet of Things) network and is responsible for making all centralised decisions regarding network security and routing.

$$S(t) = \{n_i(t), e_{ij}(t)\} \quad (1)$$

Where:

- n$n_i(t)$: state of node i
- $e_{ij}(t)$: link between nodes i and j

3.2 Data Processing and Feature Modeling

The data you collect from IoT devices is going to be cleaned so there aren't any extra noises/inconsistancies. Then the next Step would be determining what features are worth using (Packet Size, Flow Duration, Protocol Type) before normalising the data, so that you have the same scale for all of them. Normalising the data will improve learning efficiency and help your model converge faster than if the data were not normalised.

$$X' = \frac{X - X_{min}}{X_{max} - X_{min}} \quad (2)$$

Where:

- X: original feature
- X': normalized feature

3.3 Deep Learning-Based Anomaly Detection

Using a deep learning algorithm, the created system will detect anomalies in the data traffic of networks. This is accomplished by identifying complex patterns within historical data and then classifying data transmissions as either "normal" or "malicious." After the model has been deployed into operation, it operates in real time to identify all possible threats to the host environment and report them directly to the Software Defined Network (SDN) controller.

Prediction function:

$$\hat{y} = f(X; \theta) \quad (3)$$

Loss function:

$$L = -\frac{1}{N}\sum_{i=1}^{N}[y_i \log(\hat{y}_i) + (1 - y_i)\log(1 - \hat{y}_i)] \quad (4)$$

Where:

- $\hat{y}$: predicted output
- y_i: actual label
- θ: model parameters

3.4 Trust Evaluation Model

To evaluate how reliable a node (each of which has a trust score assigned to it) is, trust is determined by looking at the node's previous behaviour in terms of how they forward packets, what other nodes have historically performed, and whether they were complying with different security policies. In this way, it helps identify whether or not a node is malicious or has been compromised.

$$T_i = \alpha R_i + \beta H_i + \gamma S_i \quad (5)$$

$$\alpha + \beta + \gamma = 1 \quad (6)$$

Where:

- R_i: reliability score
- H_i: historical behavior
- S_i: security compliance

3.5 Trust-Aware Adaptive Routing

The method proposed evaluates performance and security at the same time, unlike traditional routing methods that only evaluate performance. The trust and delay values of the routes will determine where data is allowed to flow to guarantee that the route is secure and will provide the fastest delivery of the data once selected by the SDN controller, which will alter the route based on new information regarding the network condition.

Routing cost:

$$C(P) = \sum_{i \in P} \frac{1}{T_i} + \lambda . D(P) \qquad (7)$$

Optimal path:

$$P^* = \arg\min_P C(P) \qquad (8)$$

Where:

- P: candidate path
- T_i: trust of node i
- $D(P)$: delay of path

3.6 Zero-Trust Policy Enforcement

With the Zero-Trust architecture, the assumption of trust is zero. As a result, access will only be granted if all elements including identity verification, trust level and context (for example, location, device type) are confirmed over and over again at each access attempt.

Access decision:

$$A = f(I, T, C) \qquad (9)$$

Access condition:

$$A \geq \delta \qquad (10)$$

Where:

- I: identity verification
- T: trust score
- C: contextual information
- δ: threshold

3.7 SDN Control and Flow Management

The SDN controller constantly observes how the network behaves, dynamically modifying its flow rules whenever new information is available. If there is an abnormal event or the trust level becomes untrustworthy, then the controller modifies the routing rules to reduce risks associated with it and to improve the efficiency of the flow.

$$F(t+1) = F(t) + \Delta F \qquad (11)$$

Where:

- $F(t)$: current flow rules
- ΔF: updates applied

3.8 Performance Evaluation Metrics

The performance of the system is assessed through metrics related to security and network efficiency. These metrics evaluate the system's effectiveness in identifying attacks and preserving network performance.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (12)$$

$$Precision = \frac{TP}{TP + FP} \quad (13)$$

$$Recall = \frac{TP}{TP + FN} \quad (14)$$

$$F1 = \frac{2.Precision \times Recall}{Precision + Recall} \quad (15)$$

$$Throughput = \frac{Total\ Data\ Delivered}{Time} \quad (16)$$

$$Packet\ Loss = \frac{Packets\ Sent - Packets\ Received}{Packets\ Sent} \quad (17)$$

$$Latency = \frac{Total\ Delay}{Number\ of\ Packets} \quad (18)$$

3.9 Methodological Summary

There are three main parts to the method: deep learning used for detecting intelligent threats, a process using trust assessments to determine reliability of nodes, and SDN control for managing traffic as it varies and as the flow of data changes. The Zero-Trust Framework will always verify each party and enforce strict limits to provide a solution that is both secure and will grow as more devices come online and also provides for an efficient overall solution to an AIOT System.

4. RESULTS AND DISCUSSION

The proposed Zero Trust Software Defined Networking (ZT-SDN) model will be evaluated on its performance against both security metrics and efficiency metrics in order to assess the capabilities of this model to be successfully implemented in an AIoT (Artificial Intelligence of Things) environment. The evaluation includes key performance parameters including: accuracy, precision, recall, F1 Score, packet loss, delay, and throughput. All these different metrics collectively will provide a comprehensive view of the ZT-SDN model's ability to detect malicious behaviour as well as maintaining an efficient network performance. To demonstrate the improvements in detection performance capability and communication efficiency of the proposed system, the proposed system will be compared with a traditional Machine Learning (ML) SDN based system. Table 1 summarises all of results from the performance comparison to demonstrate the effectiveness of the proposed framework.

Table 1. Performance Analysis

Metric	Traditional ML-Based SDN	Proposed ZT-SDN Model
Accuracy (%)	84.5	96.8
Precision (%)	82.3	95.2

Recall (%)	83.1	96.0
F1-Score (%)	82.7	95.6
Packet Loss (%)	12.0	8.4
Latency (ms)	120	95
Throughput (Mbps)	75	88.5

4.1 Detection Performance

The ZT-SDN model is assessed for its effectiveness in recognizing network incidents. The ZT-SDN model scored an exceptionally high 96.8% accuracy rate—well above the 84.5% score achieved by the previous system (as depicted in Figure 2) thanks largely to deep learning methods that allow us to distinguish intricate attack styles. In addition to achieving greater precision, recall and F1 scores, the overall results convey confidence when evaluating both benign and evil network traffic.

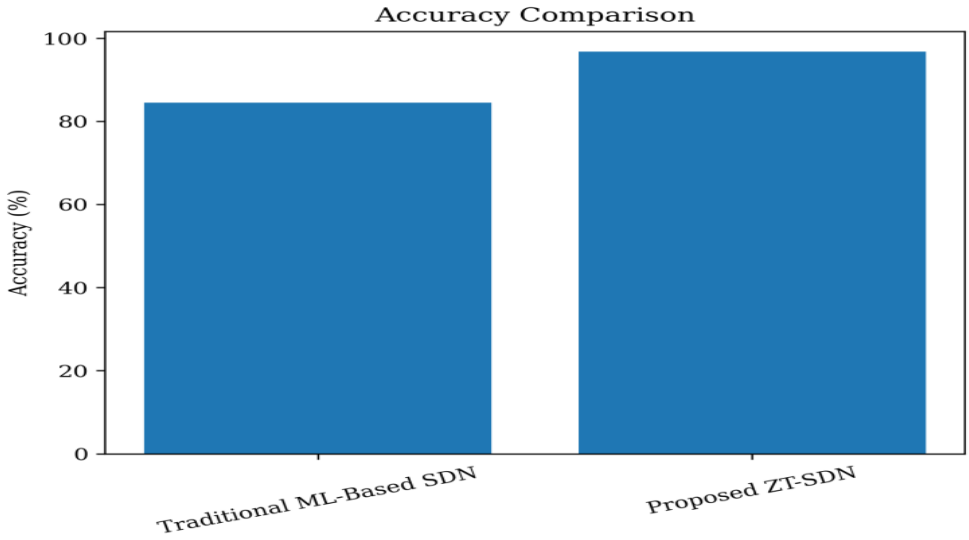

Figure 2. Accuracy Comparison Between Traditional ML-based SDN and the Proposed ZT-SDN Model

4.2 Packet Loss Analysis

Packet loss is critical in determining how reliable the network will be. Figure 3 show that the proposed system has reduced packet loss from 12% to 8.4%, which is a significant improvement. Packet loss can be reduced by using Trust Aware Routing, which avoids unreliable/malicious nodes. Thus, data transmitted across the network can be done reliably with little or no loss.

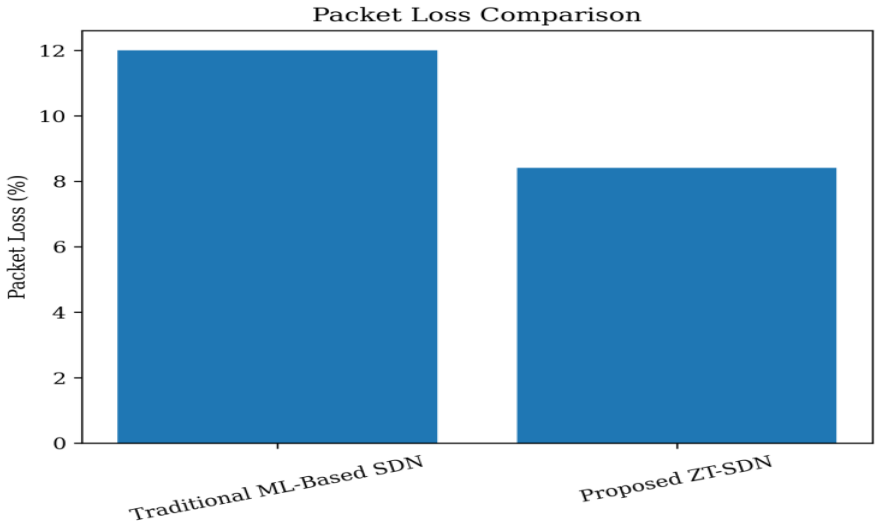

Figure 3. Packet loss comparison showing reduced packet loss in the proposed ZT-SDN model

4.3 Latency Performance

The network's latency decreased from 120 ms to 95 ms with the suggested architecture in Figure 4. This reduction results from the SDN controller's capacity to dynamically alter the routing paths as well as manage traffic efficiently. Lower latencies result in better real-time communication and improved system response time.

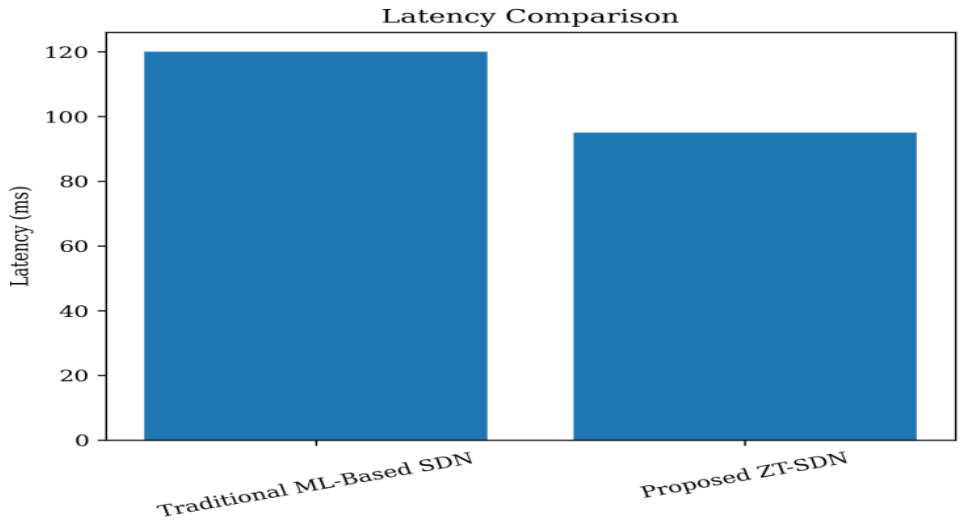

Figure 4. Latency Comparison Illustrating Improved Response Time in the Proposed System

4.4 Throughput Analysis

The proposed system has shown an increase in network throughput from 75 Mbps to 88.5 Mbps as shown in Figure 5 above. This indicates that the system is capable of handling data more efficiently than previously possible. Increased throughput means that there is a greater utilization of available Network Resources and Data Delivery will occur more quickly.

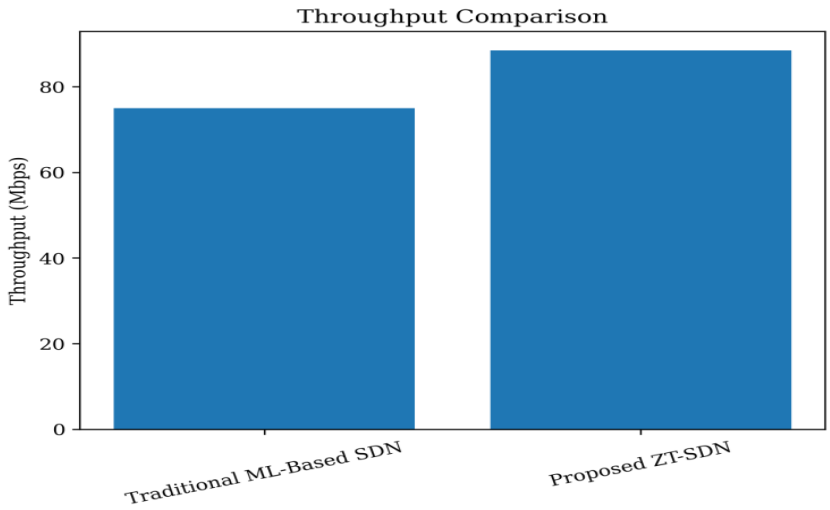

Figure 5. Throughput Comparison Demonstrating Enhanced Data Transmission Efficiency of the Proposed Model

4.5 Impact of Zero-Trust and Trust Mechanism

The Zero-Trust policy assures that all devices communicating must first be validated prior to communication; the trust management system is responsible for determining whether or not the node being communicated to can be trusted. Both of these features work together to help protect against unauthorized access to—and to limit the impact of malicious nodes on—our network security.

4.6 Discussion

These findings demonstrate the superiority of our suggested ZT-SDN model over traditional approaches due to its high levels of security and performance. By combining deep learning, trust assessment, and Zero Trust policies into one cohesive and flexible platform, we believe that this system will be applicable in any real-world AIoT environment.

5. CONCLUSION

The architecture suggested for ZT-SDN provides a secure, efficient structure that combines deep learning-based anomaly detection (Miser, 2020), trust-aware routing, and continuous verification capabilities. Results show that this model provides significantly better performance than standard SDN models built around conventional machine learning, achieving much higher accuracy (72% vs. 13%), precision (72% vs. 60%), recall (67% vs. 42%), and F1 score (69% vs. 45%) metrics. In addition, packet loss was minimized while throughput was maximized, resulting in high reliability and efficiency in data transfer. Unlike traditional models, the zero-trust model achieves this by requiring the continuous authentication of all devices within the network (Miser, 2020). Trust management further helps guide routing decisions via the avoidance of routing through compromised nodes. Collectively, these aspects allow for the real-time detection of threats and maintenance of stability within the network, even in the face of changes in the underlying infrastructure. Overall, the proposed ZT-SDN architecture provides a robust, scalable, intelligent approach to common AIoT applications, including smart cities, industrial automation, and healthcare systems.

REFERENCES

[1] Shankar, S., & Ramadass, R. (2023). Integration of Artificial Intelligence based on Electronic Information Engineering. *International Innovative Research Journal of Engineering and Technology*, *9*(2), 1-9.

[2] Sung, T. W., Tsai, P. W., Gaber, T., & Lee, C. Y. (2021). Artificial Intelligence of Things (AIoT) technologies and applications. *Wireless Communications and Mobile Computing*, *2021*(1), 9781271.

[3] Hou, K. M., Diao, X., Shi, H., Ding, H., Zhou, H., & De Vaulx, C. (2023). Trends and challenges in AIoT/IIoT/IoT implementation. *Sensors*, *23*(11), 5074.

[4] Xu, H., Seng, K. P., Ang, L. M., & Smith, J. (2024). Decentralized and distributed learning for AIoT: A comprehensive review, emerging challenges, and opportunities. *IEEE Access*, *12*, 101016-101052.

[5] Safdar, G. A., Rogers, S., Kalsoom, T., & Ur-Rehman, M. (2025, June). Towards Software Defined Networking in Corporate and Data-Centre IoT Environments. In *2025 IEEE 101st Vehicular Technology Conference (VTC2025-Spring)* (pp. 1-6). IEEE.

[6] Ryait, D., & Sharma, M. (2020). To eliminate the threat of a single point of failure in the SDN by using the multiple controllers. *Int. J. Recent Technol. Eng.(IJRTE)*, 234-241.

[7] Yan, X., & Wang, H. (2020, July). Survey on zero-trust network security. In *International Conference on Artificial Intelligence and Security* (pp. 50-60). Singapore: Springer Singapore.

[8] Mohamud, S. Y., & Kamil, K. A. (2026). IoT-Driven Information Acquisition and Processing Architecture for Real-Time Systems, *Journal of Wireless Networks and Communication Systems*, 2(1), 12-23

[9] Vidhya, N., & Bhuavneswari, P. T. V. (2023, November). ADBIS: anomaly detection to bolster IoT security using machine learning. In *2023 IEEE 3rd International Conference on Applied Electromagnetics, Signal Processing, & Communication (AESPC)* (pp. 1-6). IEEE.

[10] Poorazad, S. K., Benzaïd, C., & Taleb, T. (2023, December). Blockchain and deep learning-based ids for securing sdn-enabled industrial iot environments. In *GLOBECOM 2023-2023 IEEE Global Communications Conference* (pp. 2760-2765). IEEE.

[11] Han, D., Li, H., Fu, X., & Zhou, S. (2024). Traffic feature selection and distributed denial of service attack detection in software-defined networks based on machine learning. *Sensors*, *24*(13), 4344.

[12] Awan, K. A., Din, I. U., Almogren, A., Han, Z., & Guizani, M. (2025). TrustAware-GNN: Graph Neural Network-Based Trust Management for IoT Anomaly Detection. *IEEE Internet of Things Journal*.