Proceedings of the 4th International Conference on Machine Learning and Automation
DOI: 10.54254/2755-2721/2026.38121

Identification and Access Control of Artificial Intelligence in Zero Trust Network Architecture

Yonglan Yuan

Engineering and Technology College, Hubei University of Technology, Wuhan, China
yuanyonglan2026@outlook.com

Abstract. With the rapid development of cloud computing, mobile office, and Internet of things, the boundary of enterprise network is increasingly blurred, and the traditional security model has been unable to deal with the threat of today's complex network. With the core principle of "never trust, always verify", zero trust architecture (ZTA) breaks the traditional security model based on network boundaries. Artificial intelligence technology provides key support for the intelligent upgrading of zero trust architecture. This paper systematically reviews the research progress in this field from four dimensions: continuous authentication, multi-source anomaly detection, dynamic trust evaluation and adaptive access control. According to the research, the AUC of the multimodal CNN-LSTM hybrid model can reach 0.92, and the federated learning takes into account both privacy protection and detection accuracy; The behavior feature fusion framework based on XGboost can effectively identify internal threats. Device activity and email attachment behavior are the key distinguishing features; The subjective logic method is highly interpretable, and the quantum inspired model provides a new tool for modeling the uncertainty of trust; At present, it still faces three major challenges: privacy protection, insufficient model interpretability and standardized interoperability. This paper establishes a four-dimensional analysis framework of AI enabling zero trust, which provides a reference for subsequent theoretical research and engineering deployment.

Keywords: Zero trust architecture, artificial intelligence, Identification, access control, Continuous certification

1. Introduction

With the rapid development of cloud computing, mobile office and Internet of things, the boundary of enterprise network is increasingly blurred, and the traditional security model has been unable to deal with the threat of today's complex network. The zero trust architecture was proposed by Forrester in 2010. Its core principle is never trust and always verify, that is, it does not trust any user, device or network by default, and each access must be strictly verified [1]. However, the implementation of the zero trust architecture faces many challenges, such as dynamic, real-time and large-scale. It is difficult to meet the security requirements in the current complex network environment simply relying on static rules and manual configuration.

© 2026 The Authors. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

DOI: 10.54254/2755-2721/2026.38121

The rapid development of artificial intelligence technology provides technical support for the intelligent upgrading of zero trust architecture. Artificial intelligence technology can learn rules from massive data, accurately realize operations such as identity recognition, anomaly detection and risk assessment, and promote the evolution of zero trust from rule driven to intelligent driven [2]. The research of Gan Yuanshuai and others shows that after the introduction of artificial intelligence decision model, the anomaly detection accuracy of zero trust system can be improved to more than 95%, and the average decision response time can be reduced by about 40% [2]. Zhao Min and others pointed out in their review that the dynamic access control based on machine learning has reduced the misjudgment rate of permissions by about 35% compared with the static rule scheme, which verified the significant improvement of AI on the performance of zero trust architecture [1].

Based on the above background, this paper systematically reviews the research status of artificial intelligence in the field of identity recognition and access control in the zero trust network architecture, constructs a classification analysis framework from four dimensions of continuous authentication, multi-source anomaly detection, dynamic trust evaluation and adaptive access control, compares the performance characteristics and application scenarios of various technical methods, and analyzes the key challenges faced at present. In order to provide theoretical reference and practical guidance for the intelligent evolution of zero trust architecture.

2. Basic theory of zero trust architecture

The article zero trust architecture defines the core logical components of zero trust architecture: policy decision point (PDP) and policy execution point (PEP) [3]. PDP is composed of policy engine and policy manager, which is responsible for making access decisions according to policy, Threat Intelligence and trust algorithm; PEP is responsible for implementing the decisions of PDP, establishing and maintaining the communication channel between the subject and resources.

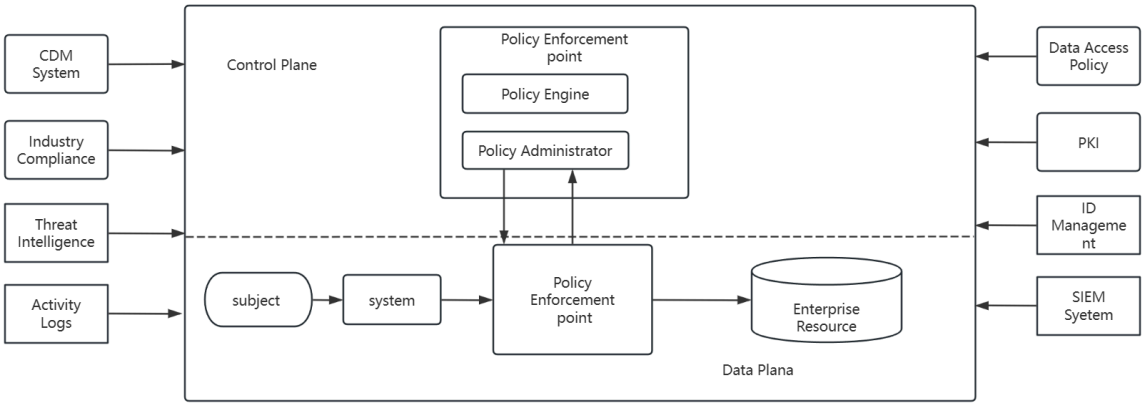


Figure 1. core zero trust logic group [3]

As shown in Figure 1, the zero trust architecture decouples security decisions from data transmission by separating the control plane from the data plane. The policy engine receives multi-source inputs from CDM system, threat intelligence, activity log, etc., and makes decisions by integrating enterprise policies and trust algorithms. This architecture realizes the transformation from border defense to identity driven.

DOI: 10.54254/2755-2721/2026.38121

In addition to the core components, the zero trust architecture also emphasizes three basic concepts, namely, identity centered, all access requests need to be authenticated and authorized, and no longer need to rely on the location of the network; With the principle of minimum permission, only the minimum permission required to complete the task is granted, and the permission is continuously evaluated during the session; Assuming that it has been breached, it does not trust any internal or external entities by default, and encrypts and monitors all traffic. According to NIST SP 800-207, the deployment path of zero trust was further defined, including the stages of asset list sorting, identity system construction, policy engine deployment and continuous monitoring optimization, which provided standardized guidance for enterprises' transformation from traditional border security to zero trust [3].

3. Application of artificial intelligence in continuous authentication

Continuous authentication is the key technology of zero trust identity recognition, which can continuously verify the user's identity during the whole session and effectively prevent the attacks of credential theft, session hijacking and other technologies. According to the technical route, it is divided into three categories: behavioral biometrics, physical layer characteristics and cryptographic protocols. Behavioral biometrics use users' unique behavior patterns (such as keyboard input habits and mouse tracks) for identity authentication, which can be continuously collected and verified without users' perception. Wang et al. Proposed a multimodal deep learning continuous authentication model, which integrates two modes of keyboard and mouse, and uses CNN-LSTM hybrid architecture, with an AUC of 0.92 [4].

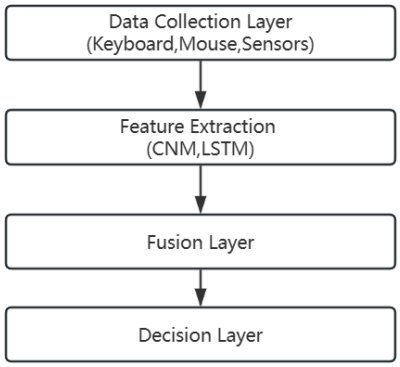


Figure 2. four layer architecture of multimodal continuous authentication model [4]

As shown in Figure 2, the multimodal model includes four levels: data acquisition, feature extraction, feature fusion and decision-making. The AIDL-XTS framework proposed by Katsis C et al. Uses mobile sensor data to authenticate through CNN-BiLSTM, and updates the trust score in real time combined with Bayesian theorem. In recent years, federated learning has also been introduced into the field of continuous authentication. Researchers have proposed a hybrid federated incremental learning framework to improve the detection rate while protecting privacy [5].

In terms of physical layer characteristics, RF fingerprint technology uses the subtle differences of signals transmitted by wireless devices for identity recognition, which is unforgeable. The two-stage unsupervised domain adaptive algorithm proposed by Jing w et al. Effectively solves the problem of RF fingerprint drift in different environments, and is suitable for Internet of things and other

DOI: 10.54254/2755-2721/2026.38121

scenarios [6]. Table 1 compares typical schemes from three dimensions: technical route, applicable scenarios and main limitations.

Table 1. Comparison of typical continuous certification schemes (table credit: original)

Programme	Technical route	Applicable scenarios	Main limitations
Multimodal deep learning	Behavioral biometrics	Desktop/office environment	Privacy concerns
AIDL-XTS	Sensor + Bayesian	Mobile/consumer electronics	rely on sensors
Radio frequency fingerprint	Physical layer characteristics	Wireless network/Internet of things	Special hardware required
5g continuous certification	Multifactor +biometrics	5g mobile communication	Process to be modified
Federated incremental learning	Federated Learning +incremental	Distributed/privacy sensitive	High communication overhead

Continuous certification has formed three main technical routes, each with its own advantages and disadvantages. Behavioral biometrics have high accuracy but have privacy risks, physical layer features are secure but need special hardware, and 5g scene scheme is deeply integrated with the network, but it is difficult to transform. Multimodal fusion and federated learning are important development directions. Continuous authentication has developed from single biometric to multimodal fusion. The use of AI technology has significantly improved the accuracy and user experience of authentication. Future development directions include multimodal feature deep fusion, federated learning privacy protection and cross device unified authentication framework [5].

Campus network scenario has the characteristics of large number of users, diverse equipment and complex behavior. The campus security defense system driven by artificial intelligence, combined with multi factor continuous authentication, abnormal behavior detection and dynamic access control, can effectively respond to threats such as account theft and exam cheating [7]. Continuous authentication is suitable for behavioral biometric schemes such as keyboard and mouse, transparent to users and without additional hardware. In 5g and industrial IOT scenarios, physical layer authentication technologies such as RF fingerprint have unique advantages, and the isolation of the network is highly consistent with the concept of zero trust micro isolation [8]. Due to the limited resources of industrial IOT devices, it is more suitable for protocol solutions such as lightweight cryptography.

From the performance comparison, the behavioral biometric scheme has the advantages of no user perception and low deployment cost, but it is easily affected by user state changes (such as fatigue and injury), and the error recognition rate is usually between 3% and 8%; The physical layer RF fingerprint scheme has high accuracy and can not be forged. It requires special signal acquisition equipment, which has high deployment cost and is limited in the application of resource constrained IOT devices; The cryptographic protocol scheme has the highest security, high computational overhead, and is difficult to achieve continuous insensible authentication. Therefore, multimodal fusion has become the current mainstream direction. By combining different characteristics, it can achieve a balance between authentication accuracy and user experience.

DOI: 10.54254/2755-2721/2026.38121

4. Application of artificial intelligence in multi-source anomaly detection

Anomaly detection is an important part of zero trust architecture. By monitoring user behavior, network traffic and system status, potential threats can be found in time. After the introduction of artificial intelligence technology, it can use massive data to train the detection model and identify more complex abnormal patterns. Suryaprakash t et al. Proposed the ztrs framework for internal threat detection based on XGBoost algorithm and behavior feature fusion [9]. The framework extracts features from multiple dimensions such as device activity, file access, e-mail use, and network communication, and uses XGBoost to train the risk scoring model. Research shows that device activity and email attachment behavior are the key factors to distinguish normal users from internal threats (Figure 3).

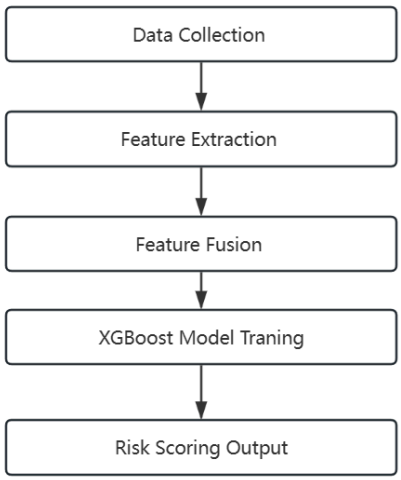


Figure 3. Zero trust risk scoring framework based on XGBoost [9]

In terms of apt and encrypted traffic detection, deep learning technology is widely used to identify typical behavior patterns of apt attacks. Aiming at the detection problems caused by the popularity of encrypted traffic, the interpretable deep learning box can accurately detect exceptions and provide interpretable results, so as to enhance the trust of operation and maintenance personnel.

From the perspective of technical classification, anomaly detection methods in zero trust scenarios can be divided into three categories: supervised learning, unsupervised learning and semi supervised learning. Supervised learning methods (such as xgboost and random forest) rely on labeled data and perform well in the detection of known threats, but the generalization ability of unknown attacks is limited; Unsupervised learning methods (such as isolated forest and self encoder) do not need to label data and can find unknown anomalies, but the false positive rate is relatively high; Semi supervised learning combines the advantages of the two and uses a small amount of labeled data to guide model training, which is a hot research direction at present. In addition, with the development of large language model technology, transformer based anomaly detection methods began to emerge, which showed potential in processing long sequence behavior data and semantic understanding. In terms of performance indicators, the artificial intelligence anomaly detection model can improve the detection accuracy to more than 95%, and reduce the average decision response time by about 40% [2].

DOI: 10.54254/2755-2721/2026.38121

5. Application of artificial intelligence in dynamic trust evaluation

Dynamic trust assessment is the core of zero trust decision-making, which continuously calculates the trustworthiness of the subject according to the multi-dimensional context. AI technology significantly improves the accuracy and adaptability of trust assessment [2]. At present, there are three main technical methods, including machine learning method, subjective logic method and quantum heuristic method. Machine learning method uses supervised/unsupervised algorithm to mine behavior characteristics and achieve high-precision trust prediction, which is suitable for IOT and big data environment. Its advantage is that it uses algorithm to dig behavior characteristics and has high prediction accuracy, which is suitable for scenes with large amount of data such as the Internet of things and big data. The disadvantage is that it has black box characteristics. The disadvantage is that the model has black box characteristics, the decision-making process is lack of explicability, it is difficult to explain the generation basis of trust score, and it is not persuasive in scenes with high security requirements (Figure 4).

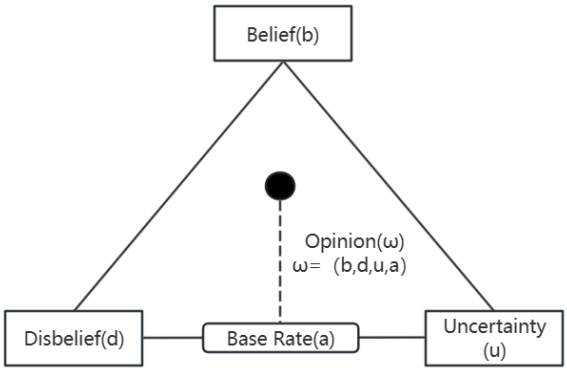


Figure 4. Three tuple representation of subjective logic trust model [10]

Katsis C and others sorted out a number of trust attributes and proposed a zero trust scoring algorithm for enterprise networks based on subjective logic. The subjective logic method uses belief, disbelief, uncertainty and relative atomic number to express trust opinions, which can clearly express uncertainty and has strong interpretability [10]. Subjective logic method has the advantage of strong interpretability, each parameter has a clear meaning, and can combine the trust opinions from multiple sources to resolve the contradiction between different evidences, which is the first choice of enterprise level zero trust scheme. Subjective logic method and machine learning complement each other, with one focusing on precision and the other on explainability. The quantum inspired trust model uses the concepts of superposition, entanglement and measurement in quantum mechanics for reference to model the uncertainty and dynamics of trust. The quantum inspired trust scoring framework proposed by Xu s et al. Uses quantum states to represent the state of trust, providing a new mathematical tool for trust modeling [11]. In terms of performance, the accuracy of trust score prediction of machine learning trust evaluation model in IOT and big data scenarios can reach more than 90%, the subjective logic method reduces the decision misjudgment rate by about 18% through explicit modeling uncertainty, and the trust score update delay of quantum inspired model remains at the sub second level [10, 11].

DOI: 10.54254/2755-2721/2026.38121

6. Application of artificial intelligence in adaptive access control

Adaptive access control is the implementation link of zero trust, which dynamically adjusts permissions according to real-time trust status. From static RBAC to dynamic ABAC, and then to context-aware ZTNA, the control grain is gradually refined (Figure 5).

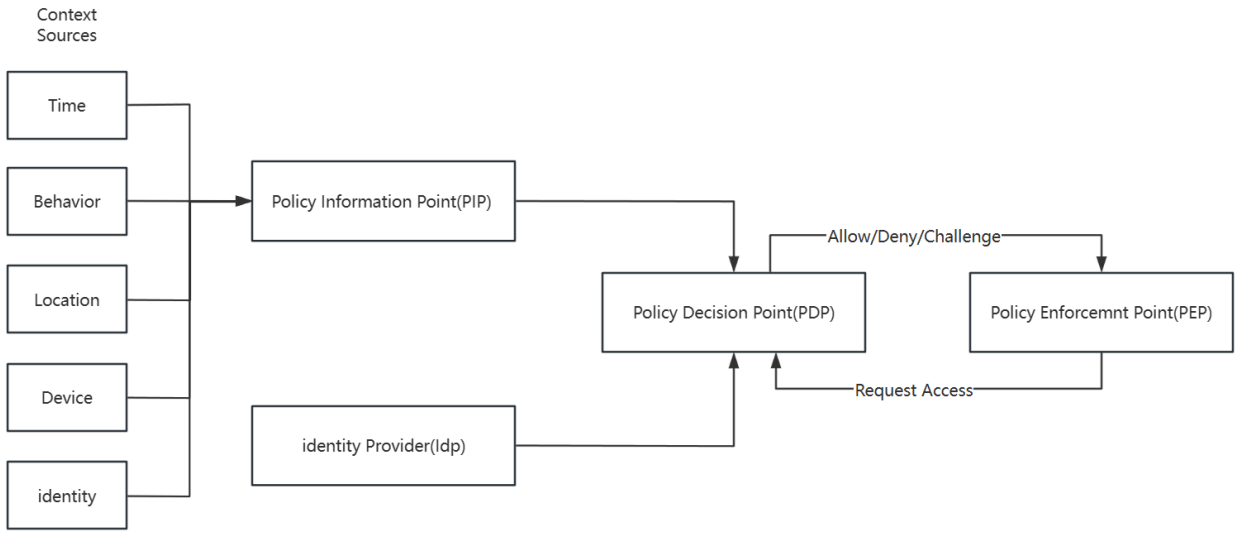


Figure 5. context aware adaptive access control architecture [12]

Context aware architecture includes three core components: identity provider, policy decision point and policy execution point. The context aware ztna scheme studied by Maameri B et al. Integrates identity, device status, location, behavior, time and other factors to achieve fine-grained dynamic control [12]. For example, access from the company network during working hours can obtain high permissions, while access from the public network during non working hours requires additional verification and permissions are limited.

In the technological evolution path, the access control model has experienced the development from discretionary access control (DAC) to mandatory access control (MAC), and then to role-based access control (RBAC). RBAC allocates permissions according to job roles. For example, it configures fixed permission sets for different roles such as administrators, ordinary employees, interns, etc., which is simple to manage, and the user permissions in the same role are completely consistent. RBAC lacks the degree of scenic spots, so it is difficult to adapt to the dynamic security requirements. Attribute based access control (ABAC) introduces multi-dimensional attributes such as user identity, device status, access location, time, resource type to judge, which significantly improves the flexibility. However, due to the large number of attributes and rules, the operation and maintenance cost is high. Ztna context aware zero trust network access is the core implementation mechanism of zero trust. It introduces real-time dynamic trust evaluation on the basis of ABAC. Permissions are no longer dependent on pre-configured static rules, but are dynamically adjusted according to the user's current trust score. When the trust level is high, permissions are relaxed, and when the trust level is low, permissions are tightened, so as to truly realize the access control goal of never trust and always verify. In terms of performance, according to the literature, compared with the static rule scheme, the dynamic access control based on machine learning reduces the misjudgment rate of permissions by about 35% [1]. The average delay of dynamic authorization decision of context aware ztna scheme is less than 50 milliseconds, which is significantly improved in security and flexibility compared with the traditional static RBAC scheme [12].

DOI: 10.54254/2755-2721/2026.38121

7. Challenges and prospects

The zero trust architecture involving artificial intelligence has made significant progress, but still faces many challenges. Privacy protection issues. The current artificial intelligence model training needs a large amount of user behavior data. Nowadays, people are more and more sensitive to the privacy issues on the network, and they are skeptical about the part of data collection. How to balance the rational use of data and the protection of users' privacy is a big challenge; The interpretability of the model is insufficient. Due to the "black box" characteristics of the deep learning model, the problem of security decision-making is difficult to explain, which affects the credibility of users to the system; Standardization and interoperability. At present, the zero trust architecture lacks a unified standard, and it is difficult for products from different manufacturers to operate with each other.

In the future, the zero trust architecture driven by artificial intelligence will develop in the direction of large language model integration, quantum security, automated operation and cross domain collaboration [2].

8. Conclusion

Aiming at the problems of identity recognition and access control faced by zero trust architecture in the intelligent upgrading, this paper systematically summarizes the research progress of artificial intelligence technology in this field, and constructs a classification analysis framework from four dimensions: continuous authentication, multi-source anomaly detection, dynamic trust evaluation and adaptive access control.

The study found that in terms of continuous authentication, multimodal fusion schemes (such as cnn-lstm hybrid architecture, AUC of 0.92) have become the mainstream direction, and the introduction of Federated learning effectively balances detection accuracy and privacy protection; In terms of anomaly detection, xgboost based behavior feature fusion framework is outstanding in internal threat detection, and device activity and email attachment behavior are the key distinguishing features; In terms of trust evaluation, the subjective logic method is highly interpretable, and the quantum inspired model provides a new perspective for trust uncertainty modeling; In terms of access control, the evolution from RBAC to ABAC and then to ztna reflects the trend of refining control granularity and enhancing context awareness.

These findings not only fill the blank of systematic review in the field of AI enabling zero trust, but also provide a reference for enterprises to choose the appropriate technical route in the actual deployment. However, this study is limited by the coverage of the literature and the availability of quantitative data, and the analysis of some emerging technologies (such as large language model fusion) is still qualitative, lacking horizontal performance comparison under a unified benchmark. Future research can further build a standardized zero trust AI evaluation benchmark, or combine new technologies such as large language model and federated learning to explore the problem of identity joint authentication and automatic policy generation in cross domain collaborative zero trust architecture.

References

[1] Zhao, M., & Qu, K. (2026). *A survey of zero trust architecture and applications.* https://link.cnki.net/urlid/31.1859.TN.20260319.1852.002

[2] Feng, Y., & Zhonghua. (2026). *Advances and challenges of artificial intelligence-enabled decision-making in zero trust.* https://link.cnki.net/urlid/32.1759.TJ.20260428.1738.014

DOI: 10.54254/2755-2721/2026.38121

[3] Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero trust architecture (NIST Special Publication 800-207). National Institute of Standards and Technology.* https://doi.org/10.6028/NIST.SP.800-207
[4] Nagarajan, S. M., Devarajan, G., Thangakrishnan, M. S., et al. (2024). Artificial intelligence-based zero trust security approach for consumer industry. *IEEE Transactions on Consumer Electronics, 70*(3), 5411-5418.
[5] Ji, J., Qiu, S., Ye, S., & Liu, X. (2026). A hybrid federated–incremental learning framework for continuous authentication in zero-trust networks. *Future Internet, 18*(3), Article 154. https://doi.org/10.3390/fi18030154
[6] Jing, W., Peng, L., Fu, H., et al. (2024). An authentication mechanism based on zero trust with radio frequency fingerprint for Internet of Things networks. *IEEE Internet of Things Journal, 11*(13), 23683-23698.
[7] Bu, Y. (2026). Design and implementation of campus network security defense system driven by artificial intelligence. *Information Recording Materials, 27*(8), 39-41. https://doi.org/10.16009/j.issn.1009-5624.2026.08.013
[8] Qiu, S., & Lin, G. (2026). 5G user continuous authentication method based on zero trust Internet of things technology. *Internet of Things Technologies, 16*(8), 31-38. https://doi.org/10.16667/j.issn.2095-1302.2026.08.007
[9] Suryaprakash, T., & Rajagopal, S. (2026). Adaptive zero trust risk scoring for insider threat detection using behavioral feature fusion and XGBoost. In *2026 3rd International Conference on Research Methodologies in Knowledge Management, Artificial Intelligence and Telecommunication Engineering (RMKMATE)* (pp. 1-5). IEEE.
[10] Katsis, C., & Bertino, E. (2025). The zero-trust paradigm: Concepts, architectures and applications. *Foundations and Trends in Privacy and Security, 8*(2), 122-253.
[11] Xu, S., & Qian, Y. (2025). Quantum-inspired trust scoring for zero trust security: A simulation-based approach. In *2025 IEEE International Conference on Quantum Computing and Engineering (QCE) (Vol. 2)* (pp. 46-49). IEEE.
[12] Maameri, B., Kenaza, T., Debicha, I., et al. (2025). Enhancing IT network security through context-aware attribute-based zero trust network access. In *2025 2nd International Conference on Advances in Electronics, Control and Communication Systems (ICAECCS)* (pp. 1-6). IEEE.