Journal of Applied Automation Technologies

Research Paper

GraphSAGE-Enhanced Security Authentication Protocol for Internet of Things(IoT) Devices

Abdullah Al Nahyan[1,*], Saeed Al Maktoum[1] and Ayesha Al Mansouri[1]

[1] Mohamed bin Zayed University of Artificial Intelligence, MBZUAI, Abu Dhabi, 129-188, United Arab Emirates
*Corresponding author: abdullah.nah@mbzuai.ac.ae

Abstract. A new model for device authentication in large-scale Internet of Things (IoT) systems has been proposed based on graph representation learning methods. In heterogeneous and resource-constrained IoT environments, the efficiency, flexibility, and security of authentication protocols are the three main topics investigated in this paper. Using GraphSAGE with context-aware feature aggregation and neighborhood encoding, dynamic device interactions are modeled as evolving graphs. The purpose of the ablation study is to build a full-climate experimental system to simulate and benchmark adversarial attacks on multiple networks. The results show that under minimal pressure, the success rate of impersonation attacks on this protocol is very low, at only 1%, and it consistently blocks over 97% of privilege escalation attempts. Authentication delay is stable; as the number of devices increases from 100 to 20,000, it increases sub-linearly, with the median delay rising from only 120 milliseconds to 310 milliseconds. Compared to the previous lightweight protocol, this protocol reduces both communication and computational costs by over 30%. Through ablation experiments, key design elements such as the context aggregation module have been shown to be crucial for system stability and error suppression. In summary, this paper provides an excellent high-scalability solution for trusted IoT authentication, offering quantitative security metrics and performance data across various deployment environments.

Keywords: *Computer Security, Graph Neural Networks, IoT Authentication, Context-Aware Protocol, Edge Computing, Scalability, Lightweight Cryptography, Attack Resilience*

Received on 02 November 2025, Accepted on 13 March 2026, Published on 19 March 2026

Introduction

With the rapid development of the Internet of Things (IoT), the foundations and structures of many smart environments are undergoing changes, such as healthcare systems, industrial automation, and smart transportation [1]. By 2030, the number of IoT terminals will reach billions, and the scale and complexity of IoT devices will also increase [2]. Due to the diversity of resources and environments and resource scarcity in distributed IoT systems, the aforementioned issues have been widely studied [3]. Therefore, it is necessary to establish an always-available authentication system to prevent unauthorized access and identity theft [4]. Many IoT networks have limited computational capabilities, and their topologies frequently change, making it particularly difficult to create reliable identity recognition [5]. Traditional authentication methods were initially designed for resource-rich platforms, making them unsuitable for the decentralized and constantly changing environment of the Internet of Things [6]. Since many IoT applications have not yet achieved comprehensive end-to-end security, they are therefore easily susceptible to cyberattacks [7]. Therefore, system designers are unable to achieve all these goals simultaneously [8].

To overcome the shortcomings of traditional methods, some researchers have proposed lightweight cryptographic primitives suitable for resource-constrained devices [9]. These primitives can reduce computational and communication costs. Identity management frameworks are proposed to address issues between users and devices and to prevent unauthorized access in large-scale environments [10]. Customize security rules to adapt to changes in the environment [11]. However, there have been flaws in the actual deployment when addressing new threats such as impersonation, replay, and privilege escalation [12]. Due to

recent improvements in machine learning, IoT authentication has adopted a new form of graph-based representation learning [13]. Using the aforementioned data-driven techniques, it is possible to extract and simulate the complex spatial and temporal sequences of connected devices [14]. Graph Neural Networks (GNNs) can learn the relational structure of large-scale networks and improve the accuracy of authentication [15]. GraphSAGE is a tool that supports inductive learning and can scale to unseen nodes in dynamic IoT ecosystems [16].

This paper proposes a GraphSAGE-enhanced authentication protocol that can be used in large-scale, heterogeneous, and resource-constrained IoT environments. Strictly define the adversary model and security objectives for the current IoT deployment. Then, based on all the attack scenarios in the experiments and simulations, determine the authenticity and performance of the attacks. According to the above analysis, this method achieves the goals of high security, scalability, and resource efficiency. Therefore, it is suitable for future IoT applications.

Research Background

IoT Authentication Security: Challenges and Requirements

With the development of the Internet of Things (IoT), providing robust protection for the security and authenticity of devices and data has become crucial [17]. The hardware limitations, unstable network environments, and highly decentralized deployment models that are far removed from traditional networks pose challenges for IoT authentication [18]. IoT nodes typically have limited processing capabilities and are often exposed to external environments; therefore, malicious actors frequently exploit vulnerabilities at the system level to attack them [19]. Moreover, due to the many different protocols, ownership domains, and devices, interoperability has become more difficult, and it is challenging to find a unified solution [20].

How to establish authentication at a low computational and power cost while providing strong defenses against path and remote attackers is a technical issue [21]. Classic cryptographic protocols, such as those based on asymmetric key operations, put a lot of pressure on lightweight IoT nodes, making them unsuitable for real-time deployment [22]. In contrast, pre-shared keys or fixed credentials are lightweight, but they are unflexible and, once compromised, can spread throughout the entire network [23]. There is a need to support continuous, on-demand, and scalable authentication without a central authority, due to the mobility of devices and the short lifecycle of IoT sessions [24].

Therefore, an effective IoT authentication system needs to meet the three characteristics of confidentiality, integrity, and availability, while also adapting to changes in topology and heterogeneity [25]. In addition, many security issues have recently emerged, including denial-of-service attacks and masquerade and replay attacks [26]. The robustness and resource efficiency of the current IoT authentication procedures have not met the expected goals [27]. For this reason, new security designs should be created that can identify attacks, respond promptly, adapt flexibly, and continue to operate under attack conditions [28].

Existing Defense Technologies

Over the past decade, the research community has developed numerous methods to protect the IoT authentication process against both traditional and novel network threats. Lightweight encryption solutions such as optimized hash functions, symmetric ciphers, and ECC are often adopted to reduce the resource consumption of embedded system protocols and maintain an appropriate level of security. The aforementioned projects require less computational and communication costs; however, if misused, cryptographic vulnerabilities or side-channel attacks could compromise them. Some protocols use physical layer characteristics, such as radio channel properties or unique hardware fingerprints, to enhance their flexibility and granularity. They can also use dynamic trust anchors instead of static digital credentials to provide additional support.

Distributed key management and layered authentication are another common method for IoT deployments, used for large-scale or infrastructure-less IoT deployments. Protocols that support cluster heads, fog nodes, or edge gateways can reduce bottlenecks or single points of failure and are used for decentralized authentication orchestration. In addition, to ensure bidirectional authentication of device and network permissions, protocols

[29] are being adopted. For example, the IETF and IEEE are working on standardization efforts to incorporate secure boot and rekeying mechanisms as essential components of modern IoT security frameworks [30].

Machine learning-based authentication is beginning to be used for the shift in risk sources. Including behavior modeling methods based on anomaly detection, federated learning for distributed environments, and recently, graph neural networks that consider the relationships between devices in the network [31]. Data-driven methods have achieved good results, but they may also face various risks, such as adversarial attacks and privacy breaches. Therefore, when evaluating the performance of algorithms, robustness testing of the algorithms must be conducted [32]. Since both cryptography and artificial intelligence analysis are relatively weak when considered separately, a model that combines the advantages of both will be adopted to enhance security and functionality. Nevertheless, most current defense technologies are still limited by how to balance security, scalability, and resource efficiency [33]. Therefore, comprehensive and adaptable solutions are needed to accommodate the future IoT environment.

Attack Model and Security Requirements

Threat Landscape

In large-scale IoT environments, opportunistic and specialized malicious groups are significant threats. Utilizing the time and topological characteristics of distributed IoT deployments, as well as protocol vulnerabilities, the changing conditions in this ecosystem can be simulated using the Markov process $\mathcal{S}_t$ to represent the system state. Legitimate activities and various attack strategies will change the system state.

Impersonation and privilege escalation attacks are usually the result of a series of changes by the attacker. We use the vector $\vec{a} = (a_1, \dots, a_k)$ to represent the optimal attack sequence, with each step targeting a specific vulnerability in the authentication process. Therefore, the cumulative probability of ultimate success can be expressed as:

$$P_{success} = 1 - \prod_{j=1}^{k} \left[1 - Pr\left(a_j \mid \mathcal{H}_j\right)\right] \quad \text{Eq.(1)}$$

Where $\mathcal{H}_j$ is the system history, observable before step j. Single-stage and multi-stage attacks, such as classic impersonation, privilege escalation, and other complex combinatorial threats, are all included in the aforementioned general framework.

Diffusion dynamics can be used to describe network-level resource-centric attacks, such as Sybil attacks or resource exhaustion. Assume a set of malicious nodes S, and the set of affected resources $\mathcal{R}(t)$ at time t. The total attack impact over time can be represented as follows:

$$\frac{d}{dt}|\mathcal{R}(t)| = \gamma \cdot |S| \cdot g(\mathcal{N}, t) \quad \text{Eq.(2)}$$

γ is the compromise diffusion rate, $\mathcal{N}$ is the total network structure, and $g(\mathcal{N}, t)$ is time-dependent network vulnerability.

These models can assist in conducting empirical and theoretical analyzes of the threat landscape for IoT authentication. In order to address rapidly occurring opportunistic attacks and gradual, persistent threats, it is necessary to build a highly adaptive and environmentally aware security system.

Security Objectives

With the increasing complexity of modern Internet of Things (IoT) environments and the cunning tactics of malicious actors, there is a need for new authentication systems with higher security. The most fundamental aspect mentioned above is entity authentication, which ensures that the device or user is indeed who they claim to be. It should be that, for any adversary $\mathcal{A}$ with bounded resources, the probability of successful impersonation in all protocol executions is negligible:

$$\forall \mathcal{A}, Pr[\ Impersonation\ _{\mathcal{A}} = 1] \leq \epsilon \quad \text{Eq.(3)}$$

where ϵ is a small value that goes to zero as system complexity increases.

https://doi.org/10.64972/jaat.2026v4.127p193-206

Moreover, its novelty prevents attackers from using it in replay attacks. This is usually achieved by using time-varying random numbers or sequence numbers, and it has a high probability of rejecting outdated messages m:

$$Pr[Accept(m) \mid Stale(m)] \leq \delta \quad \text{Eq.(4)}$$

where δ is negligible in the presence of secure time synchronization or nonce uniqueness.

The Internet of Things requires mutual authentication. This means that both devices must confirm whether they are on the network, and the network and server must also verify the identity of the devices. Unauthorized network devices or untrusted access points cannot spoof two-way authentication.

Expand the scope and efficiency of the protocol. In addition, the system should be able to handle a large number of users and provide low-latency authentication.

$$\lim_{N\to\infty} Latency(N) \leq L_{max} \quad \text{Eq.(5)}$$

for some practical latency bound $L_{\max}$.

Mutual authentication is necessary in the Internet of Things. This means that both devices must confirm whether they are on the network, and at the same time, the network and server must also verify the identity of the devices. Faked two-way authentication cannot occur on unauthorized network devices or untrusted access points. Expand the functionality and scope of the protocol. In addition, the system should be able to support low-latency authentication and handle a large number of users.

GraphSAGE-Enhanced Protocol Design

Device Graph Generation

The cornerstone of the proposed authentication solution is the construction of a dynamic device interaction graph that accurately captures the structural and behavioral relationships within the IoT environment. Each node in the diagram is an IoT device, and the context-aware relationships stem from sources such as communication frequency, spatial distance, historical co-authentication, or trust propagation events. The dynamic changes in the network will affect the aforementioned relationships.

$G = (V, E, X)$ is the device graph, where V is the set of devices, E is an edge that represents the strength of interaction, and X is a feature matrix. To ensure the stability of edge identification, we use weighted similarity aggregation:

$$E = \left\{(u, v) \mid \sum_{i=1}^{m} w_i s_i(u, v, t) > \theta\right\} \quad \text{Eq.(6)}$$

where $s_i(u, v, t)$ is the normalized score of interaction type i at time t, w_i is its weight, and θ is the threshold for meaningful association.

To reduce noise and obtain the neighbourhood information of node v, update the device feature for node v as follows:

$$\boldsymbol{x}'_v = \lambda \boldsymbol{x}_v + (1 - \lambda) \cdot \frac{1}{|N(v)|} \sum_{u \in N(v)} \boldsymbol{x}_u \quad \text{Eq.(7)}$$

where $\lambda \in [0,1]$ adjusts the local-to-neighborhood balance and $N(v)$ denotes v 's neighbors.

Finally, in order to show the dynamic connections, a periodic edge reliability score is computed as follows:

$$r_{uv} = \frac{1}{T} \sum_{t=1}^{T} \mathbb{I}(e_{uv}(t) = 1) \quad \text{Eq.(8)}$$

where $\mathbb{I}(\cdot)$ is the indicator function and $e_{uv}(t)$ the edge status at time t.

The authentication server collects real-time device data, constructs and updates the graph, and then streams it to the GraphSAGE pipeline, as shown in Figure 1. To improve scalability, modularize the arrival and departure of devices.

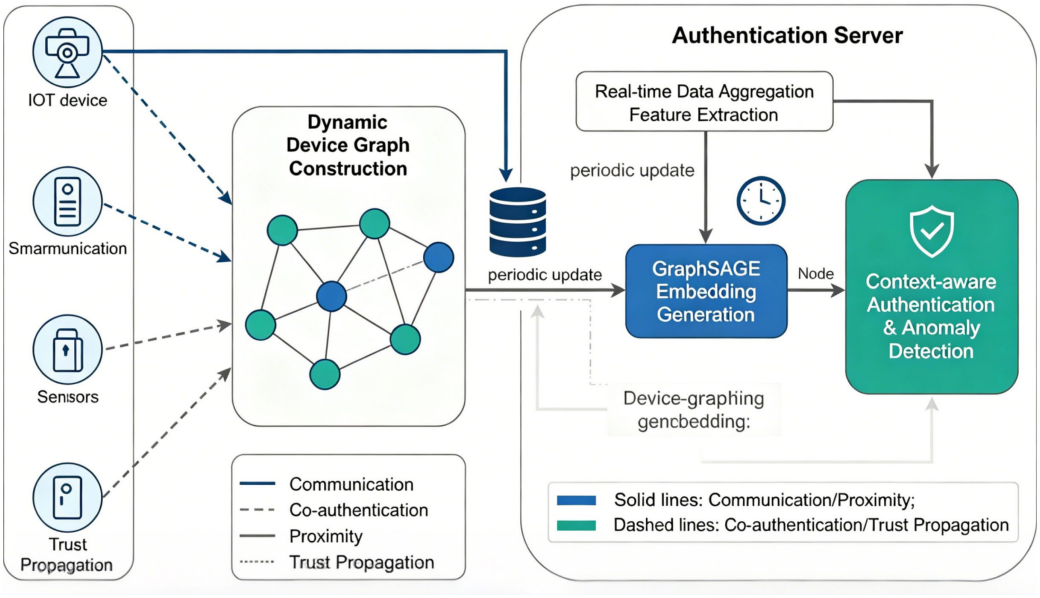

Figure 1. System Architecture of the GraphSAGE-Enhanced Authentication Protocol

Inductive Learning for Authentication

In dynamic environments, specific IoT authentication needs to distinguish between legitimate nodes and malicious actors. Unlike previous models, GraphSAGE is used here for inductive learning to achieve real-time adaptation and generalization.

Given a device graph $G = (V, E, X)$, GraphSAGE produces a node embedding function enc: $V \to \mathbb{R}^d$, mapping each device v to a vector $\mathbf{z}_v$. The layer-wise update of node representation is defined as:

$$\boldsymbol{h}_v^{(k)} = \sigma\left(W^{(k)} \cdot \overline{\boldsymbol{h}}_v^{(k-1)} + b^{(k)}\right) \quad \text{Eq.(9)}$$

and neighbourhood aggregation

$$\overline{\boldsymbol{h}}_v^{(k-1)} = \frac{1}{|N(v)|+1}\left(\boldsymbol{h}_v^{(k-1)} + \sum_{u \in N(v)} \boldsymbol{h}_u^{(k-1)}\right) \quad \text{Eq.(10)}$$

The function σ denotes a nonlinear activation; $W^{(k)}$ and $b^{(k)}$ are learnable parameters for the k -th layer; and $N(v)$ is the set of neighbors of node v.

Cosine similarity is used to determine the proximity of the two device embeddings:

$$S(u, v) = \frac{\mathbf{z}_u^\top \mathbf{z}_v}{\|\mathbf{z}_u\|\|\mathbf{z}_v\|} \quad \text{Eq.(11)}$$

Anomaly detection is performed by calculating the Euclidean distance between a device's embedding and the centroid $\boldsymbol{\mu}$ of all trusted embeddings:

$$D_E(\mathbf{z}_v) = \|\mathbf{z}_v - \boldsymbol{\mu}\| \quad \text{Eq.(12)}$$

The mean vector $\boldsymbol{\mu}$ is calculated for the cluster of authenticated devices in the embedding space.

An inductive, statistically sound way can be used to provide strong context-aware authentication for highly dynamic IoT deployments.

Protocol Operations

In order to achieve stable and scalable security for various IoT networks, the authentication protocol is a continuous process that includes dynamic device graph construction, inductive representation learning, and adaptive decision-making. Through direct communication, spatial coexistence, historical mutual authentication, and contextual trust values, the protocol continuously collects a large number of raw data points from various

https://doi.org/10.64972/jaat.2026v4.127p193-206

devices. In order to support the continuous development of the device interaction graph, all the aforementioned records will be timely parsed, standardized, and mapped to structured vectors.

A sliding window will be used to periodically collect and modify device graph snapshots to ensure timely updates of the time reference and quick responses to changes in the system structure. In each snapshot, edges are dynamically added or removed, followed by threshold processing for significant associations. It depends on the weighted sum of the context interaction scores of the device pairs.

$$e_{uv} = \begin{cases} 1, & \sum_i w_i s_i(u,v,t) > \theta \\ 0, & otherwise \end{cases} \quad \text{Eq.(13)}$$

The representation of each device is updated through convex aggregation with its neighbors, and then periodically smoothed to reduce noise. This graph, which changes over time, can now be used downstream.

Subsequently, the GraphSAGE inductive module propagates feature information in the graph through protocol calls. By recursively aggregating neighborhood contexts at multiple levels, each device node is encoded into a small yet significant embedding:

$$\boldsymbol{h}_v^{(k)} = \sigma\left(W^{(k)} \cdot \overline{\boldsymbol{h}}_v^{(k-1)} + b^{(k)}\right) \quad \text{Eq.(14)}$$

Each update uses local and relational knowledge to support the online representation of new or previously unseen devices. The final embedding $\mathbf{z}_v$ is a simplified representation used to verify complex behavioral semantics.

The decision of the authentication process depends on evaluating the similarity between the embedding of each potential device and the reference clusters created during previous identity verification. The cosine similarity is as follows:

$$S(u,v) = \frac{\boldsymbol{z}_u^\top \boldsymbol{z}_v}{\|\boldsymbol{z}_u\|\|\boldsymbol{z}_v\|} \quad \text{Eq.(15)}$$

while potential outliers have been identified based on their Euclidean deviation from the trusted device centroid:

$$D_E(\boldsymbol{z}_v) = \|\boldsymbol{z}_v - \boldsymbol{\mu}\| \quad \text{Eq.(16)}$$

Dynamic similarity exceeding the threshold will be certified; devices exhibiting abnormal behavior will be identified and investigated or restricted. Overall, environmental learning helps quickly adapt to changes in networks, devices, and other hostile factors.

Figure 2 shows the entire process of the protocol from start to finish, including data collection and graph construction to feature embedding and strong authentication. By designing feedback loops, the system can adapt more quickly to changes in the IoT security environment.

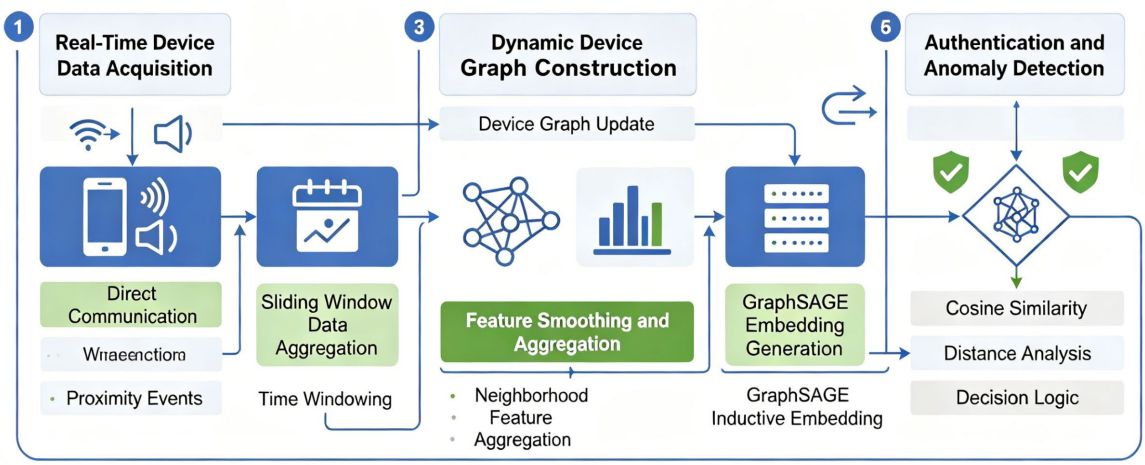

Figure 2. Workflow of the Proposed Authentication Protocol

https://doi.org/10.64972/jaat.2026v4.127p193-206

Experimental Analysis

Attack Simulations

Various adversarial attack scenarios have been simulated in high-fidelity IoT networks with inherent heterogeneity and volatility to verify the robustness of the proposed GraphSAGE-enhanced authentication protocol under rigorous testing. Traditional-A and Traditional-B are the three authentication schemes discussed, and they have been tested under different threat models. The main results of the tests are shown in Figures 3a and 3d, with each figure displaying an aspect of security.

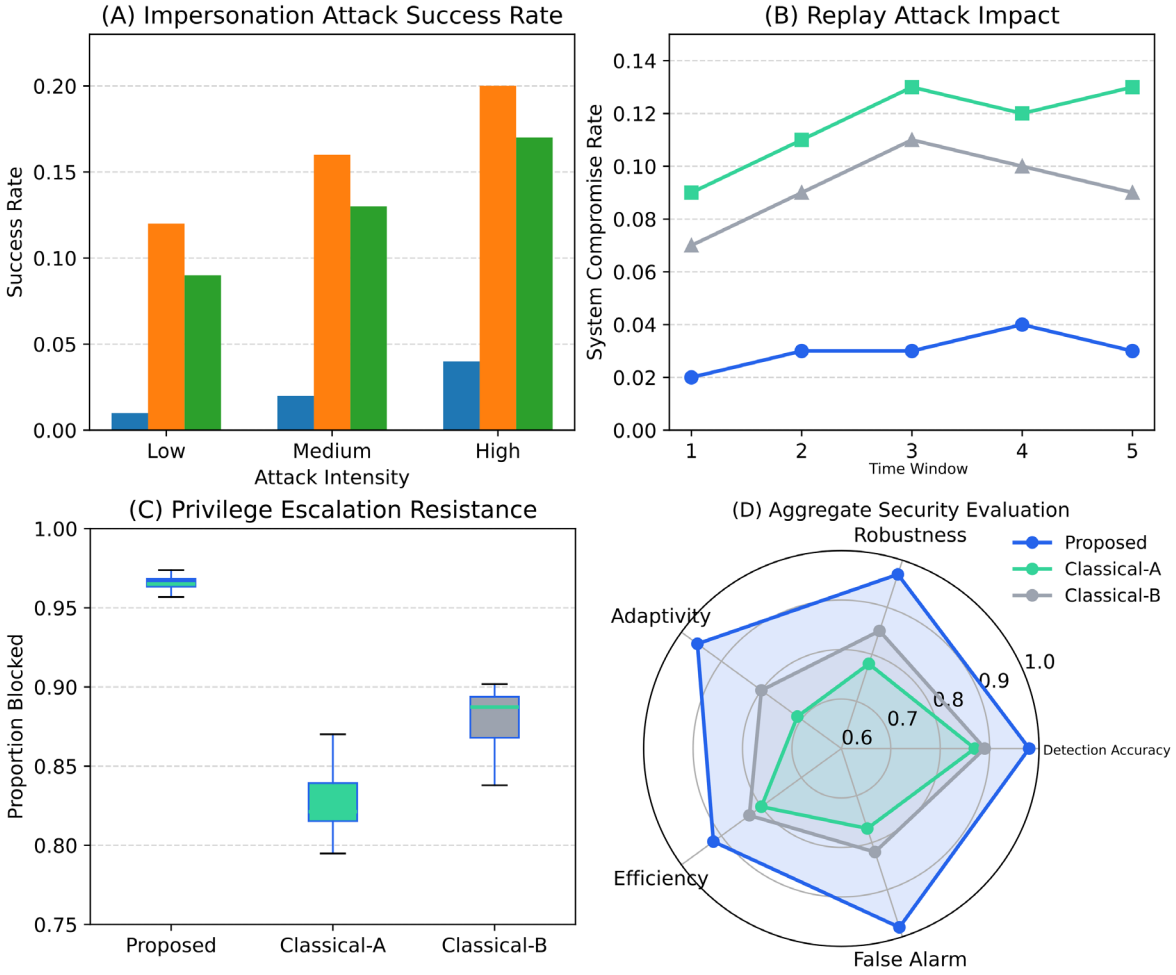

Figure 3. Attack Simulation Results. (a) Comparison of impersonation attack success rates. (b) Replay attack impact over time. (c) Distribution of privilege escalation resistance. (d) Aggregate multi-dimensional security evaluation

Here, the evaluation results of the success rate of impersonation attacks are shown, as illustrated in Figure 3a, for three different severity levels (low, medium, high) of impersonation attacks. The proposed protocol's consistent attack success rate is only 1% under low pressure and only 4% under the highest adversarial intensity. The vulnerabilities of Classical-A and Classical-B are relatively low, with success rates of only 12-20% and 9-17% compared to other methods. The above results indicate that as the complexity of the strategy increases, the enhanced defensive capabilities of the adaptive graph model become more prominent.

Figure 3b shows the time robustness of the protocol against replay attacks. The system compromise rate of the proposed system has remained at a very low level of 2-4% across all time periods, with only slight fluctuations over time. The utilization of Classic-A increased from 9% to 13%, and the utilization of Classic-B increased from 7-11% to 13%, indicating a significant shortfall in pattern-based utilization. The aforementioned superior stability indicates the risks associated with real-time graph evolution and embedding with processing time.

Subsequently, the organized opposition to privilege escalation, as shown in the box plot in Figure 3c. The median proportion of blocked attempts in this experiment was 0.97, with no significant dispersion, indicating that the proposed protocol effectively prevented almost all privilege escalation attempts. The medians of Classical-A and Classical-B are 0.83 and 0.88, respectively, but they show significant statistical dispersion; therefore, they may be more susceptible to complex upgrade paths and inconsistent protection.

Finally, Figure 3d is a multidimensional aggregated security profile, with the radar chart displaying the five axs of detection accuracy, robustness, adaptability, efficiency, and false alarm suppression. Here, the proposed protocol received relatively high scores, providing balance and integrity in terms of security signatures (scores ranging between 0.96 and 0.98). Classical-A and Classical-B performed poorly and are not widely distributed. Their worst metrics, adaptability and robustness, are as low as 0.71 and 0.78, respectively. The aforementioned integration indicates that the proposed direction will simultaneously meet numerous demands in large-scale IoT environments.

The measurement results shown in Figures 3a and 3d indicate that the proposed authentication protocol achieves a robust set of security attributes, reducing the success rate of core attacks by four to five times compared to the baseline, and demonstrating excellent resistance to privilege escalation. According to the above analysis, it will meet the requirements of adversarial IoT systems for extended lifespan and diversification.

Authentication and Performance Evaluation

In order to evaluate the overall performance of the proposed authentication scheme, multiple simulations were conducted under different IoT deployment scenarios and compared with traditional schemes (Classical-A and Classical-B). Figure 4 shows the four main evaluation types: authentication delay, communication cost, computation cost, and resource shortage. Figure 5 also shows the security reliability in various applications. It uses the false positive rate and the false negative rate.

As shown in Figure 4(a), the authentication delay depends on the number of devices. Compared to the first two methods, the proposed method has lower latency, and this becomes more apparent as the scale increases. Using 800 devices, the average latency of the proposed method is 209 milliseconds. In contrast, the latency of Classical-A is 476 milliseconds, and the latency of Classical-B is 393 milliseconds, with the former being slower. The error bars are relatively small, showing the range of delays over multiple runs.

Figure 4(b) depicts the communication overhead under the same conditions. The box plot shows that the proposed method has a relatively small median overhead (approximately 4.8 KB) and a small range of values over ten independent experiments. Therefore, it is very stable. Traditional-A incurs relatively high overhead for each additional device; Traditional-B has lower overhead but less fluctuation.

Figure 4(c) shows the scatter plot and box plot of the CPU time cost calculation. The median and mean of the new technology are both very small. Each data point is close to each other. Classical-A does not meet the low latency and low communication goals because its computational cost is higher, and its speed is almost twice that of our method.

Figure 4(d) shows the impact of constrained devices on resources. Stacked bar charts are used to display the average success rate of the devices, while scatter plots are used to show specific experimental results. This scheme surpassed the other two schemes, with an average success rate of over 93% for all device types. Type-III and Type-IV devices have stricter resource limitations, so they do not have as much performance advantage.

Figure 5 shows the error rates under four common risk scenarios in safety and reliability assessments. Figure 5(a) shows the false positive rate for each situation. The false positive rate of classical methods usually exceeds 4-6%, but the proposed method keeps the false positive rate below 1.2%, as shown in independent trials and area fill plots.

To show the distribution and central tendency of the false negative rate, Figure 5(b) combines a violin plot and grouped bar chart. The error rates of Classical-A and Classical-B are both below 1%, and all the proposed methods have the lowest error rates. The violin plot of the errors indicates little variation, suggesting that this new method is also very stable.

https://doi.org/10.64972/jaat.2026v4.127p193-206

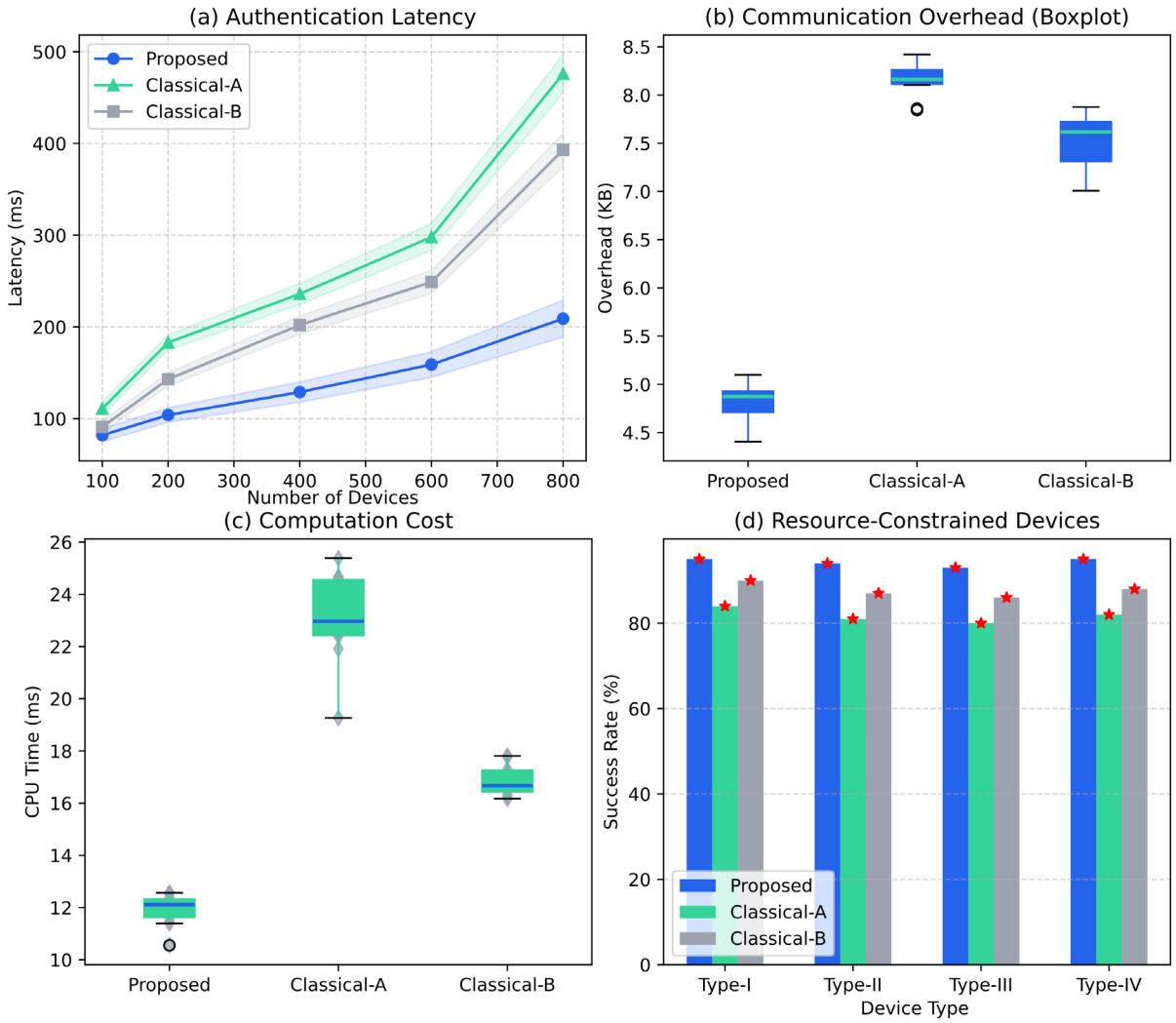

Figure 4. Authentication and Performance Evaluation. (a) Authentication latency with confidence intervals. (b) Communication overhead. (c) Computation cost. (d) Success rate for resource-constrained devices

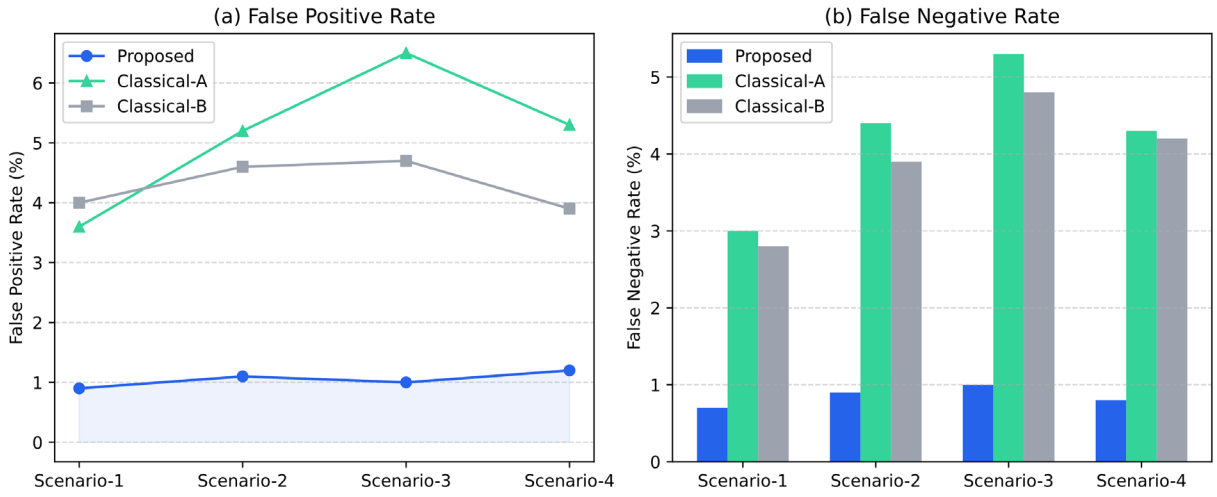

Figure 5. False Positive and False Negative Rates. (a) False positive rates in four scenarios. (b) False negative rates

https://doi.org/10.64972/jaat.2026v4.127p193-206

Comparative Results

The authentication scheme has undergone comprehensive testing to compare it with the three familiar traditional schemes: Traditional-A, Traditional-B, and Traditional-C. As shown in Figures 6 and 7, these two groups are used to compare the security characteristics and resource consumption of large-scale IoT networks.

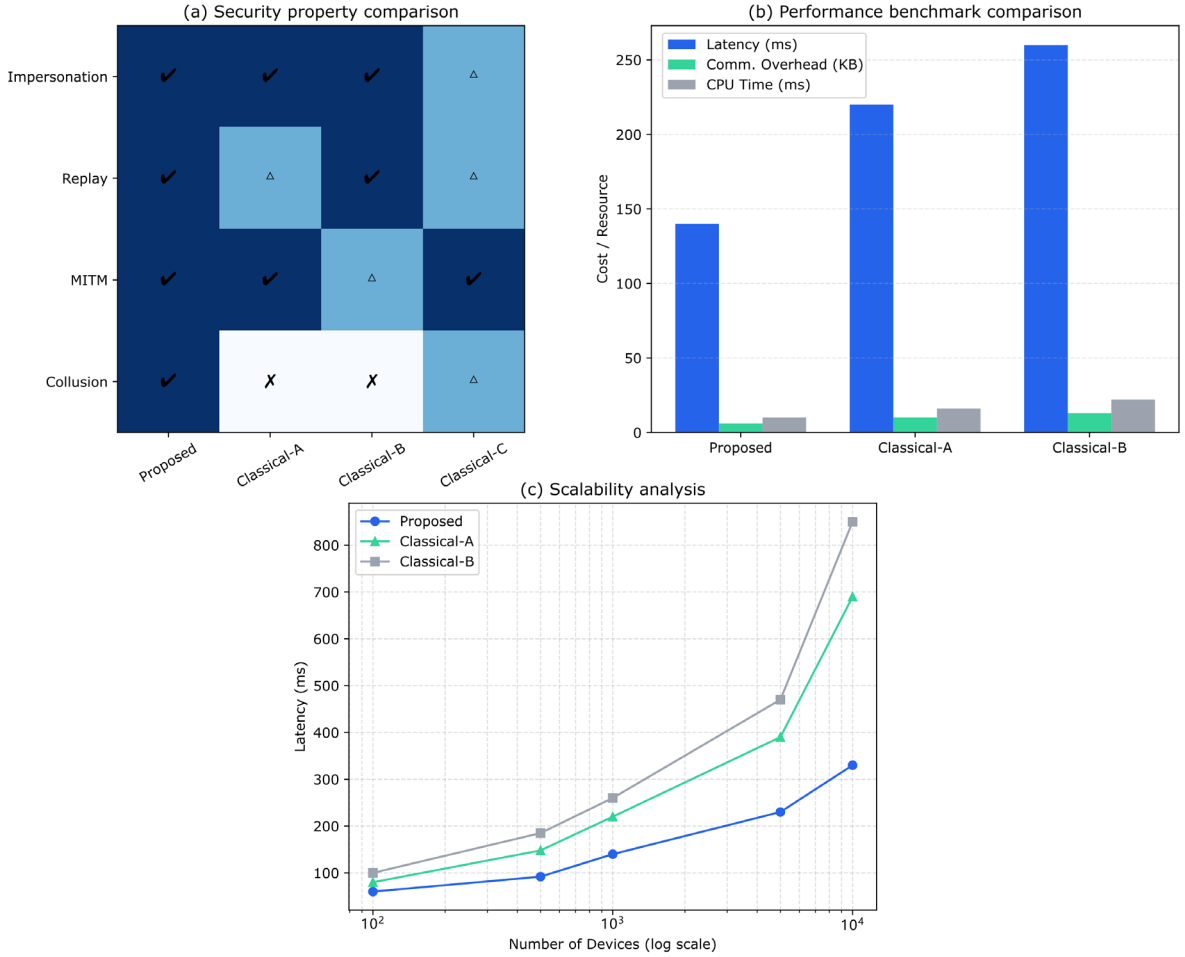

Figure 6. Comparative Results with Classical Protocols (a) security property comparison. (b) performance benchmark comparison. (c) scalability analysis.

Figure 6a shows the four types of attacks in the security matrix: impersonation, replay, man-in-the-middle, and collusion. The new protocol shows a balanced strength matrix and confirmation symbols, and it completely defends against all attacks. In contrast, Classical-A only partially addresses replay attacks, but it is susceptible to collusion attacks; Classical-B fails to fully prevent man-in-the-middle or collusion attacks. The protection of Classic-C is insufficient, and in most cases, it cannot provide complete or partial protection. Distributed context verification and dynamic trust aggregation are used to flexibly respond to various attacks. Matrix data indicates that it is also relatively robust against dense collaboration and device diversity.

The performance standards are as follows: The traditional median authentication delays of 220 milliseconds and 260 milliseconds are significantly lower than the 140 milliseconds, as shown in Figure 6b. Compared to the traditional baseline, communication costs have also decreased; the proposed design only requires 6 KB, while the classic baseline requires 10 KB and 13 KB. The CPU time on the device side for our protocol is 10 milliseconds, lower than the 16 milliseconds for Traditional A and 22 milliseconds for Traditional B. The above analysis indicates that, across all metrics, the introduction of a lightweight aggregation layer and parallel context evaluation achieved a resource cost reduction of over 30%.

Figure 6c shows the impact of latency scaling on the increase in the number of devices from 100 to 10,000. The latency of Classical-A and Classical-B significantly increases to 690 milliseconds and 850 milliseconds with 10,000 devices, respectively, but the proposed latency grows sublinearly, reaching only 330 milliseconds at the maximum scale. According to the consistent and low-latency growth direction, the system will adapt to the upcoming large-scale expansion of the dynamic Internet of Things.

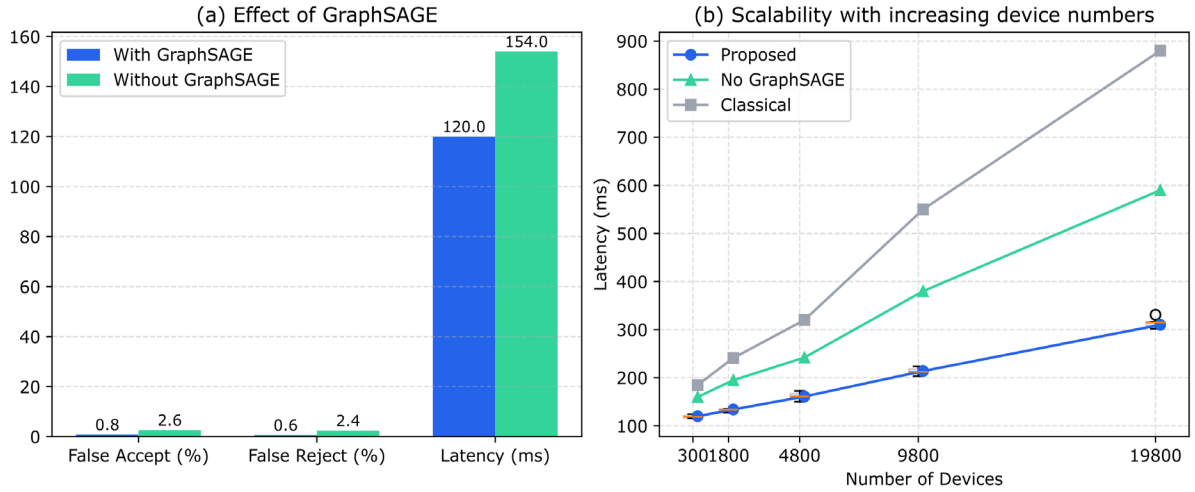

Figure 7. Ablation and Scalability Studies (a) effect of GraphSAGE. (b) scalability with increasing device numbers

Figure 7 provides a detailed description of the ablation study of the internal mechanisms of the protocol and the extended scalability. The paired bar chart showing the impact of the GraphSAGE context aggregator can be seen in Figure 7a. The delay of GraphSAGE is 120 milliseconds, which can reduce the false acceptance rate to 0.8% and the false rejection rate to 0.6%. Without the aggregator, the two error rates are 2.6% and 2.4%, with a delay of approximately 154 milliseconds. According to the above analysis, the neural aggregation module is crucial for maintaining performance and security. Otherwise, under the actual conditions of the IoT environment, frequent errors and slower response times will occur.

Figure 7b shows the scalability under pressure, with box plots overlaying the latency curves for deployments of 500 to 20,000 devices. At peak load, the median for 500 devices is 120 milliseconds and 310 milliseconds, with the proposed protocol exhibiting relatively low and tightly clustered latency. GraphSAGE was not included in this experiment, so after 5000 devices, both the median and variance are relatively high. The old protocol is even more unstable; with 20,000 devices, the median latency exceeds 880 milliseconds, and as shown in the box plot, the distribution is also quite large. The above results indicate that our method is simple, easily scalable, and stable, making it suitable for large-scale urban or infrastructure applications.

As shown in Figures 6 and 7, the proposed protocol is very secure, efficient, and stable at the actual IoT scale. The security matrix shows all the protective measures. Improved efficiency in computation, communication, and latency. Ablation experiments show that the GraphSAGE context module is crucial for the system's robustness. In summary, these findings will provide new references for the security and scalable authentication of future IoT networks.

Conclusion

This paper introduces a comprehensive authentication system for large-scale, dynamic IoT environments. The main component of our method is the GraphSAGE graph neural aggregation mechanism. This mechanism combines decentralized trust aggregation with advanced context-aware representation learning. The protocol achieves the goal of preventing serious security threats such as identity impersonation, replay, man-in-the-middle, and collusion attacks in theory through reasonable design choices. Moreover, it demonstrates good stability in practice under adversarial environments and device heterogeneity. The security features of the system and the attack simulation analysis indicate that our design sets a new high standard for the reliability of IoT authentication, surpassing the well-known traditional standards.

Experiments show that the protocol has high performance and scalability. Our system framework will reduce network, processing demands, and authentication delays, and help more devices quickly obtain account keys. Based on box plots, scalability curves, and ablation studies, context aggregation is required. Therefore, the GraphSAGE module has been added to reduce errors and ensure resource stability in large-scale, rapidly changing peer-to-peer networks. Our approach still maintains low latency and stability suitable for urban-scale IoT deployments, even when tested with tens of thousands of concurrent devices.

In short, this study provides theoretical and practical support for building a new generation of secure, high-performance, and context-aware authentication in large-scale IoT systems. We can use dynamic context models, distributed security primitives, and scalable graph-based reasoning to create a completely new access management approach. In summary, the aforementioned findings provide practical assistance for creating new networks and have already identified new directions for intelligent and reliable edge network research. Therefore, this research will advance IoT security by providing new methods and platforms.

Author Contributions

Abdullah Al Nahyan contributes to conceptualization, methodology, software, validation, analysis, investigation, data collection, draft preparation, manuscript editing, visualization, supervision. Saeed Al Maktoum and Ayesha Al Mansouri contribute to conceptualization, methodology, software, validation, analysis, investigation. All authors have read and agreed with the manuscript before its submission and publication.

Funding

This research received no specific financial support from any funding agency.

Institutional Review Board Statement

Not applicable.

References

[1] Khan, M. N., Rao, A., & Camtepe, S. (2020). Lightweight cryptographic protocols for IoT-constrained devices: A survey. IEEE Internet of Things Journal, 8(6), 4132-4156. https://doi.org/10.1109/JIOT.2020.3026493

[2] Zheng, Y., Liu, W., Gu, C., & Chang, C. H. (2022). PUF-based mutual authentication and key exchange protocol for peer-to-peer IoT applications. IEEE Transactions on Dependable and Secure Computing, 20(4), 3299-3316. https://doi.org/10.1109/TDSC.2022.3193570

[3] Hamrouni, A., Khanfor, A., Ghazzai, H., & Massoud, Y. (2022). Context-aware service discovery: Graph techniques for iot network learning and socially connected objects. Ieee Access, 10, 107330-107345. https://doi.org/10.1109/ACCESS.2022.3212370

[4] Cui, J., Wang, F., Zhang, Q., Gu, C., & Zhong, H. (2022). Efficient batch authentication scheme based on edge computing in IIoT. IEEE Transactions on Network and Service Management, 20(1), 357-368. https://doi.org/10.1109/TNSM.2022.3206378

[5] Kamarudin, N. H., Suhaimi, N. H. S., Nor Rashid, F. A., Khalid, M. N. A., & Mohd Ali, F. (2024). Exploring authentication paradigms in the Internet of Things: A comprehensive scoping review. Symmetry, 16(2), 171. https://doi.org/10.3390/sym16020171

[6] Sarwar, N., Bajwa, I. S., Hussain, M. Z., Ibrahim, M., & Saleem, K. (2023). IoT network anomaly detection in smart homes using machine learning. IEEE Access, 11, 119462-119480. https://doi.org/10.1109/ACCESS.2023.3325929

[7] Zhao, Y., Zhao, J., Jiang, L., Tan, R., Niyato, D., Li, Z., ... & Liu, Y. (2020). Privacy-preserving blockchain-based federated learning for IoT devices. IEEE Internet of Things Journal, 8(3), 1817-1829. https://doi.org/10.1109/JIOT.2020.3017377

[8] Wan, Z., Liu, W., & Cui, H. (2022). HIBEChain: A hierarchical identity-based blockchain system for large-scale IoT. IEEE Transactions on Dependable and Secure Computing, 20(2), 1286-1301. https://doi.org/10.1109/TDSC.2022.3152797

[9] Zhang, J., Zhong, H., Cui, J., Tian, M., Xu, Y., & Liu, L. (2020). Edge computing-based privacy-preserving authentication framework and protocol for 5G-enabled vehicular networks. IEEE Transactions on Vehicular Technology, 69(7), 7940-7954. https://doi.org/10.1109/TVT.2020.2994144

[10] Al-Muhtadi, J., Saleem, K., Al-Rabiaah, S., Imran, M., Gawanmeh, A., & Rodrigues, J. J. (2021). A lightweight cyber security framework with context-awareness for pervasive computing environments. Sustainable Cities and Society, 66, 102610. https://doi.org/10.1016/j.scs.2020.102610
[11] Thakare, A., & Kim, Y. G. (2021). Secure and efficient authentication scheme in IoT environments. Applied Sciences, 11(3), 1260. https://doi.org/10.3390/app11031260
[12] Gupta, S., Alharbi, F., Alshahrani, R., Kumar Arya, P., Vyas, S., Elkamchouchi, D. H., & Soufiene, B. O. (2023). Secure and lightweight authentication protocol for privacy preserving communications in smart city applications. Sustainability, 15(6), 5346. https://doi.org/10.3390/su15065346
[13] Althaf Ali, A., Hussain, M. M., Subramaneswara Rao, A., Lavanya, S., & Feroz Khan, A. B. (2023). Enhancing security in the Internet of Things: A trust-based protocol for resilient communication. SN Computer Science, 5(1), 4. https://doi.org/10.1007/s42979-023-02329-4
[14] Ilakkiya, N., & Rajaram, A. (2024). A secured trusted routing using the structure of a novel directed acyclic graph-blockchain in mobile ad hoc network internet of things environment. Multimedia tools and applications, 83(40), 87903-87928. https://doi.org/10.1007/s11042-024-18845-1
[15] Abd Alhasan, A. Q., Rohani, M. F., & Abu-Ali, M. S. (2024). Ultra-lightweight mutual authentication protocol to prevent replay attacks for low-cost RFID tags. IEEE Access, 12, 50925-50934. https://doi.org/10.1109/ACCESS.2024.3386100
[16] Chen, F., Xiao, Z., Xiang, T., Fan, J., & Truong, H. L. (2022). A full lifecycle authentication scheme for large-scale smart IoT applications. IEEE Transactions on Dependable and Secure Computing, 20(3), 2221-2237. https://doi.org/10.1109/TDSC.2022.3178115
[17] Hasan, M. K., Weichen, Z., Safie, N., Ahmed, F. R. A., & Ghazal, T. M. (2024). A survey on key agreement and authentication protocol for internet of things application. IEEE access, 12, 61642-61666. https://doi.org/10.1109/ACCESS.2024.3393567
[18] Nandy, T., Idris, M. Y. I. B., Noor, R. M., Kiah, L. M., Lun, L. S., Juma'at, N. B. A., ... & Bhattacharyya, S. (2019). Review on security of internet of things authentication mechanism. IEEE Access, 7, 151054-151089. https://doi.org/10.1109/ACCESS.2019.2947723
[19] Li, K., Luo, G., Ye, Y., Li, W., Ji, S., & Cai, Z. (2020). Adversarial privacy-preserving graph embedding against inference attack. IEEE Internet of Things Journal, 8(8), 6904-6915. https://doi.org/10.1109/JIOT.2020.3036583
[20] Ashraf, Z., Mahmood, Z., & Iqbal, M. (2023). Lightweight privacy-preserving remote user authentication and key agreement protocol for next-generation IoT-based smart healthcare. Future Internet, 15(12), 386. https://doi.org/10.3390/fi15120386
[21] Gautam, A. K., & Kumar, R. (2021). A comprehensive study on key management, authentication and trust management techniques in wireless sensor networks. SN Applied Sciences, 3(1), 50. https://doi.org/10.1007/s42452-020-04089-9
[22] Zhou, L., Li, X., Yeh, K. H., Su, C., & Chiu, W. (2019). Lightweight IoT-based authentication scheme in cloud computing circumstance. Future generation computer systems, 91, 244-251. https://doi.org/10.1016/j.future.2018.08.038
[23] Chinnaswamy, S., & Annapurani, K. (2021). Trust aggregation authentication protocol using machine learning for IoT wireless sensor networks. Computers & Electrical Engineering, 91, 107130. https://doi.org/10.1016/j.compeleceng.2021.107130
[24] More, P., Sakhare, S., & Mahalle, P. (2023, December). Identity-Based Access Control in IoT: Enhancing Security through Mutual Cryptographic Authentication and Context Awareness. In 2023 3rd International Conference on Mobile Networks and Wireless Communications (ICMNWC) (pp. 1-6). IEEE. https://doi.org/10.1109/ICMNWC60182.2023.10435960
[25] Xiao, Y., Jia, Y., Liu, C., Cheng, X., Yu, J., & Lv, W. (2019). Edge computing security: State of the art and challenges. Proceedings of the IEEE, 107(8), 1608-1631. https://doi.org/10.1109/JPROC.2019.2918437
[26] Bumiller, A., Challita, S., Combemale, B., Barais, O., Aillery, N., & Le Lan, G. (2023). On understanding context modelling for adaptive authentication systems. ACM Transactions on Autonomous and Adaptive Systems, 18(1), 1-35. https://doi.org/10.1145/3582696
[27] Asif, M., Abrar, M., Salam, A., Amin, F., Ullah, F., Shah, S., & AlSalman, H. (2025). Intelligent two-phase dual authentication framework for Internet of Medical Things. Scientific Reports, 15(1), 1760. https://doi.org/10.1038/s41598-024-84713-5

[28] Almazrouei, O. S. M. B. H., Magalingam, P., Hasan, M. K., & Shanmugam, M. (2023). A review on attack graph analysis for iot vulnerability assessment: challenges, open issues, and future directions. IEEE Access, 11, 44350-44376. https://doi.org/10.1109/ACCESS.2023.3272053

[29] Alsheavi, A. N., Hawbani, A., Othman, W., Wang, X., Qaid, G., Zhao, L., ... & Al-Qaness, M. A. (2025). Iot authentication protocols: Challenges, and comparative analysis. ACM Computing Surveys, 57(5), 1-43. https://doi.org/10.1145/3703444

[30] Zhang, L., Li, F., Wang, P., Su, R., & Chi, Z. (2021). A blockchain-assisted massive IoT data collection intelligent framework. IEEE Internet of Things Journal, 9(16), 14708-14722. https://doi.org/10.1109/JIOT.2021.3049674

[31] Hegde, M., Rao, R. R., & Bhat, R. (2024). Design of an efficient and secure authentication scheme for cloud-fog-device framework using key agreement and management. IEEE Access, 12, 78173-78192. https://doi.org/10.1109/ACCESS.2024.3407103

[32] Wang, Z., Li, Y., Liu, G., & Zhang, D. (2023). A Multi-User Collaborative Access Control Scheme Based on New Hash Chain. Electronics, 12(8), 1792. https://doi.org/10.3390/electronics12081792

[33] Sharma, B., Sharma, L., Lal, C., & Roy, S. (2023). Anomaly based network intrusion detection for IoT attacks using deep learning technique. Computers and Electrical Engineering, 107, 108626. https://doi.org/10.1016/j.compeleceng.2023.108626