Intelligent Multimedia Processing & Communication Systems Journal

IMPCSJ

J IMPCS (2025) 19: 9-20
DOI 10.71856/IMPCS.2025.1209110

Research Paper

A Novel Security-by-Design Framework Based on the XMPP Protocol for Intelligent Communications in the Internet of Things

Hamid Doustali[1], Mir Ali Seyyedi[2*], Behzad Lak[3]

1. PhD student in Information Technology Management, Department of computer engineering, S&R.C., Islamic Azad University, Tehran, Iran
2. Assistant Professor, Department of Computer Engineering, ST.C., Islamic Azad University, Tehran, Iran.
**Corresponding Author*
3. Assistant Professor, Department of Computer Engineering, Amin University, Tehran, Iran

Article Info

Article history:
Received: 11 Jan 2025
Accepted: 20 Feb 2025

Keywords:
Fault tolerance,
Internet of Things,
Security-by-design,
Trust management,
XMPP.

ABSTRACT

This article presents a lightweight and federated framework for securing intelligent communication in the Internet of Things (IoT) scope, based on the Extensible Messaging and Presence Protocol (XMPP) with a security-by-design approach. The core innovation lies in embedding security mechanisms within the message-oriented XMPP layer without requiring dedicated hardware, while maintaining full compatibility with resource-constrained devices. The proposed approach integrates TLS/SASL encryption, a dynamic trust management layer, with real-time updates, and capability-based access control. Three threat scenarios message injection, identity spoofing, and DoS attacks have been simulated in the Python environment. Results present that the system achieves 98% privacy preservation, 96% authentication success rate, 87% fault tolerance, an average power consumption of 83 Mw, and a handshake delay of 44 Ms demonstrating significant improvement over baseline methods. These metrics reflect a well-balanced trade-off between security and performance in heterogeneous IoT networks, indicating that the XMPP-SBD framework is a practical solution for scalable and secure IoT deployment.

I. Introduction

The Internet of Things (IoT) refers to a pervasive network of physical objects equipped with sensors and actuators that exchange data via the internet. Estimates suggest that the number of these devices will exceed tens of billions within the current decade, encompassing everything from smart homes to critical infrastructure [1, 2]. The real-time connectivity of data within this ecosystem enables opportunities such as process optimization and personalized services; however, it simultaneously broadens the surface for cyberattacks. The core functionality of IoT relies on low-power, reliable communication among heterogeneous nodes. Constraints related to packet size, processing power, and energy consumption have led to the adoption of lightweight protocols such as CoAP, MQTT, and XMPP in place of conventional internet communication standards [1,3]. Nevertheless, these very limitations impose additional challenges in ensuring the confidentiality, integrity, and availability of data, thereby necessitating security mechanisms tailored to resource-constrained environments [4, 5].

With the rapid expansion of IoT in critical sectors such as healthcare, energy, and transportation, the need to secure communication between devices has become more urgent than ever. Some Studies have emphasized the importance of lightweight protocols like XMPP in safeguarding data [1, 2]. This research aims to propose a secure, lightweight, and implementable framework that accounts for real-world threat scenarios, including injection attacks and identity spoofing. The research assumptions are grounded in the heterogeneity of processing capabilities and energy constraints among IoT nodes. The study's relevance arises from the performance gap between security and efficiency in existing approaches. By integrating access control, adaptive trust layers, and encryption, this work introduces an innovative approach to security-by-design in IoT systems.

The "security-by-design" paradigm seeks to embed protective mechanisms into system architecture prior to deployment. In this study, the federated, message-oriented XMPP protocol was chosen as the communication backbone due to its native support for TLS encryption, SASL authentication, and cross-domain scalability [1,2]. The combination of these capabilities with message signing and trust management establishes a framework in which confidentiality, authentication, and access control are maintained from the implementation layer through to the application layer [6].

Numerous studies have proposed security frameworks for IoT. For example, the VIRTUS middleware enables secure event exchange within private networks [1], while XEP-0027, coupled with SAML/SASL, strengthens communication among federated cloud systems [2]. Hardware-based frameworks such as ASSURE leverage Physical Unclonable Functions (PUFs) to reduce energy consumption [7], and PSAF-IoT combines Elliptic Curve Cryptography (ECC) with unclonable functions to deliver lightweight authentication [8].

Despite these advancements, many solutions either require dedicated hardware or impose significant computational overhead on resource-constrained devices. Moreover, the majority of prior research has focused on protocols like MQTT or CoAP, with limited exploration of the federated and scalable capabilities of XMPP.

The remainder of this paper is organized as follows: The related work and literature review section discusses existing studies on secure IoT communication, evaluating their strengths and limitations. The Materials and Methods section introduces the proposed framework based on XMPP and the security-by-design approach, detailing its communication, security, and access control layers, as well as the Python-based simulation environment and attack scenarios. The Results and Discussion section presents performance metrics—such as privacy preservation, access control effectiveness, and fault tolerance—and compares them with existing solutions. Finally, the Conclusion and Future Work section summarizes key findings and outlines potential directions for further research

II. Related works

With the rapid proliferation of the Internet of Things, security challenges such as authentication, privacy preservation, and encrypted communication have emerged as central issues in the design of communication systems. The XMPP, as a real-time communication solution, offers features such as authentication, encryption, and scalability for IoT environments [1]. For instance, the VIRTUS middleware leverages XMPP to implement a security structure based on the TLS and SASL, enabling secure and event-driven data exchange among devices within private distributed networks [1].

In the domain of cloud security, Klesti et al. proposed a federated architecture employing XEP 0027 extensions and single-sign-on authentication mechanisms such as SAML/SASL to establish a secure cross-domain communication framework that ensures message integrity and user privacy [2]. In the context of wireless sensor networks, the hybrid MG-Net model—combining GRU and MobileNet—enhances intrusion detection accuracy while reducing energy consumption. In this architecture, trust establishment is handled via the EigenTrust algorithm, and secure communication is facilitated through the DTLS protocol [3].

Choi et al. introduced a two-dimensional (2D) framework to ensure end-to-end security from IoT applications to devices. This model integrates symmetric encryption and attribute-based security with uniquely assigned device identities—an especially critical approach for sensitive applications such as healthcare [4]. In line with this, the Sharelock protocol was proposed by Lizardo et al. to support secure group communication using post-quantum-resistant encryption, tailored for low-cost IoT devices [5].

Yu et al., in a registered patent, introduced a method for encrypting IoT data by assigning unique keys and identities to each data packet [6]. The security framework proposed by Bhardwaj incorporates vulnerability analysis, secure protocols (TLS/DTLS), and anomaly detection systems implemented, throughout the device development lifecycle [7]. Similarly, Hamed et al. presented a comprehensive behavioral traffic identification model that leverages machine learning algorithms and security-focused design principles to detect executable malware in IoT [8].

The integration of MQTT with the ARIA-256 encryption algorithm and the mbedTLS library has strengthened data transmission security, mitigating threats such as eavesdropping, data tampering, and unauthorized access [9]. Likewise, the PSAF-IoT framework combines Physical Unclonable Functions (PUFs) and Elliptic Curve Cryptography (ECC) to provide lightweight authentication mechanisms for IoT devices [10].

Sahami et al. proposed a dual-layer encryption protocol based on MQTT using AugPAKE and PRESENT algorithms, which supports mutual authentication and ensures message integrity [11]. Within the IoTAC framework, Siavas et al. incorporated the concept of security-by-design for IoT software, offering a comprehensive security model through continuous security monitoring during various development phases [12].

Loganathan and Jaganathan optimized MQTT using the Seagull evolutionary algorithm, achieving improvements in energy consumption, latency, and packet delivery ratios [13]. In energy-constrained devices such as smart meters, Anani and Odeh developed the lightweight and secure wM-Bus security protocol based on the Noise Framework, significantly extending device lifespan while preserving communication security [14].

The IoT-Crypto framework employs a digital certificate architecture and DTLS-based communication to provide an efficient and secure solution for encryption and authentication in IoT networks [15]. A key challenge in IoT lies in its structural divergence from traditional networks (e.g., wireless sensor networks), where there are no clearly defined boundaries between internal and external users. In this regard, King-Lacroix, in his doctoral dissertation, introduced decentralized protocols like StarfishNet and BottleCap, offering distributed security architecture for access control and encrypted communication [16].

In the realm of blockchain-based IoT security, Bayani and Karoun proposed a patented platform based on a multilayered blockchain structure (including event and device chains), demonstrating how smart contracts and token-based mechanisms can preserve data integrity [17]. From a hardware perspective, Yilmaz et al. designed the ASSURE protocol, which uses PUFs and symmetric encryption to achieve superior performance and reduced energy consumption compared to DTLS [18].

For critical applications like healthcare, Akshata et al. introduced the lightweight Xor-HMAC encryption method for MQTT, which eliminates the need for SSL/TLS and reduces resource usage [19]. Sengupta and Kando emphasized the importance of secure hardware design by analyzing hardware threats such as Trojans and reverse engineering, recommending IP block-level protections like digital watermarking and obfuscation [20].

New standards such as EDHOC and Group OSCORE, introduced by Höglund et al., aim to reduce message sizes and simplify key exchange in constrained environments, outperforming DTLS in terms of efficiency [21]. To mitigate public-key encryption overhead, Hooman et al. proposed three lightweight extensions for the HIP DEX protocol, including session resumption and Denial-of-Service protection mechanisms [22].

Chaduvula et al. developed a collaborative design framework called Secure Codesign, which enables secure optimization without exposing sensitive information [23]. Hossain Khan and Patnaik combined JSON Web Tokens (JWT) with unique private keys to develop a secure identity verification solution for Google IoT Core, suitable for resource-limited devices [24].

The security framework by SMH et al. places special emphasis on the perception layer (sensors), offering a hardware-based solution using PUF and FPGA technologies to ensure data confidentiality and authenticity [25]. In the power sector, Song et al. utilized TrustZone and OP-TEE mechanisms to develop application authentication procedures for deployment on smart grid devices [26].

Dandotia and Gupta, in their systematic review, analyzed the advantages and limitations of lightweight cryptographic, hashing, and authentication protocols in IoT security frameworks [27]. In heterogeneous environments, Nguyen et al. proposed a secure and lightweight communication scheme based on CoAP, DTLS, and AES, supplemented with a decentralized VPN solution [28]. The IoTAttest framework, introduced by Derin et al., uses TPM 2.0 and remote attestation technologies to ensure the integrity of data and devices in critical environments [29].

Finally, Liu and Ji, analyzing peer-to-peer protocols, proposed two novel two-factor authentication methods based on the Chord architecture and cryptography, leading to reduced response times and memory consumption [30].

While prior research has significantly advanced IoT security, a federated and lightweight framework based on XMPP that fully integrates security-by-design principles has yet to be developed. Many existing solutions either depend on dedicated hardware and intensive computation—rendering them incompatible with the limited resources of IoT devices—or lack dynamic trust management and fine-grained access control mechanisms capable of responding in real time to internal threats.

Moreover, comprehensive evaluations of the trade-offs between security and performance—especially in terms of privacy, energy consumption, and latency—under realistic threat scenarios such as message injection, identity spoofing, and Denial-of-Service (DoS) attacks remain scarce. The present study addresses these gaps by introducing the XMPP-SBD framework, which holistically combines federated communication, lightweight cryptographic protocols, and a security-by-design approach tailored for constrained IoT environments.

TABLE I: Comparison of Related Studies with the Proposed XMPP-Based Framework Incorporating Security-by-Design Principles

Reference	Key Contributions	Challenges	Comparison with Present Study
[3]	Development of a trust-based Intrusion Detection System (IDS) for network security.	Weakness in addressing injection and spoofing attacks at the routing layer.	By simulating application-layer attacks and analyzing key security indicators, the present study offers a more comprehensive evaluation than previous works.
[5]	Implementation of end-to-end encryption for group communication in IoT.	Exclusive focus on group communication; lacks operational evaluation such as delay and energy metrics.	The proposed model in this article quantitatively evaluates not only communication security, but also delay, energy consumption, authentication success rate, and fault tolerance.
[7]	Proposal of an intelligent security framework for Industrial IoT	Complex architecture and reliance on numerous components in industrial IoT environments.	The proposed framework is lightweight, modular, and deployable on resource-constrained devices; implemented in a Python simulation environment.
[2]	Integration of XEP-0027 with SAML/SASL for federated authentication.	High complexity in implementing Single Sign-On (SSO); ineffective on low-resource devices.	This study presents a lightweight and practically deployable framework for real-world environments with low power consumption.
[1]	Introduction of an XMPP-based architecture for secure communication in IoT.	Lack of support for dynamic authentication and trust management.	In the proposed model, secure communication is complemented by an adaptive trust layer and role-based access control.

III. Proposed Approach

To design a secure communication framework for the Internet of Things (IoT) based on the XMPP protocol, a security-by-design approach was adopted. Rather than incorporating security mechanisms after system development, this approach integrates them from the early stages of communication architecture design. The objective is to ensure data integrity, confidentiality, and authentication across all communication layers. TABLE II presents the simulation environment.

TABLE II: Detailed Description of Assumptions and Simulation Settings

Component / Title	Detailed Description
Node Resource Constraints	All IoT nodes in the simulation environment are modeled with limitations in processing power, memory, and energy.
Security Scenarios	Three types of attacks—message injection, identity spoofing, and Denial-of-Service (DoS)—are modeled.

Communication Protocol	The XMPP protocol, secured with TLS encryption and SASL authentication, is employed as the primary communication layer.
Access Control	A Capability-Based Access Control (CBAC) model is used to manage permissions.
Dynamic Trust Management	A time-based and adaptive trust management system is implemented among nodes in the network.
Message Exchange and Data Logging	All nodes periodically send and receive messages; cumulative data is stored throughout the simulation.
Performance Evaluation Metrics	Key metrics assessed include privacy preservation, authentication success rate, latency, energy consumption, and fault tolerance.
Simulation Language and Tools	All implementations are carried out in Python using the Google Colab environment.
Data Generation Algorithms	Synthetic data is generated using Normal, Poisson, Gamma, and Uniform distributions.
Visualization Tools	Radar charts, ROC curves, CDFs, histograms, violin plots, and heatmaps are generated and saved using Matplotlib.
System Evaluation Criteria	Metrics such as handshake success rate, CPU temperature, reliability, encryption error rate, and communication stability are extracted.
Controlled Simulation Conditions	Scenarios are executed over uniform time intervals under repeatable conditions to ensure result reliability.
Comparative Framework Versions	Three framework versions (S1, S2, S3) with varying configurations are used for comparative analysis.
Generalizability	The designed environment is compatible with the constraints and heterogeneity characteristic of real-world IoT networks.

The XMPP was selected as the communication backbone in this study due to its federated architecture, which enables robust cross-domain communication—an essential feature for the heterogeneous nature of IoT environments [1, 2]. Features such as TLS-based encryption and SASL-based authentication allow for the establishment of a secure channel for data exchange between devices [1]. Moreover, XMPP's message-oriented structure and support for native encryption make it a suitable choice for secure and scalable communication, justifying its adoption in this research. To reinforce the security posture of the proposed framework, additional layers for encryption and message signing were integrated into the architecture. The use of protocols such as SAML/SASL is recommended for implementing message signing and single-sign-on (SSO) authentication in federated environments [2]. Furthermore, a trust management layer was implemented, utilizing lightweight algorithms such as EigenTrust to evaluate node reputations and detect both internal and external threats across the network [3, 7, 10].

The proposed framework comprises three main layers:

Communication Layer: Communication between nodes is established through the XMPP protocol. The TLS module is employed for encryption, while SASL handles authentication.

Internal Security Layer: This layer incorporates modules for intrusion detection based on deep learning, dynamic trust management, and digital message signing [3, 8, 13].

Access Control and Policy Enforcement Layer: This component utilizes a capability-based access control approach, similar to bottle cap, ensuring that only nodes with valid credentials can gain access to sensitive resources [16].

Figure 1 illustrates the architecture of the proposed method. In this study, a lightweight and deployable framework is presented for securing data exchange in IoT networks. Utilizing simulated data, various attack scenarios are modeled and evaluated. Implementation and simulation are conducted in a Python environment, with a focus on two primary threats: message injection and identity spoofing. Ultimately, the security performance of the protocol is assessed using key indicators such as privacy preservation, access control enforcement, and fault tolerance.

The proposed approach differs fundamentally from prior work in that it embeds security mechanisms directly into the message-oriented XMPP layer from the architectural design phase—eliminating the need for specialized hardware. It incorporates dynamic trust management and capability-based access control to enable real-time mitigation of internal threats. This design achieves a well-balanced trade-off between security and performance under realistic scenarios. The core contribution of this research is the integration of security-by-design principles with the federated architecture of XMPP, enabling secure and low-overhead communication in constrained IoT environments. TABLE III presents the hardware and software specifications of the simulated IoT nodes. The simulation environment closely mirrors real-world resource-constrained nodes, ensuring the practical relevance of the results. The use of RIOT-OS and TLS 1.3 implementation guarantees applicability to industrial and medical domains. Additionally, the choice of the Sleek XMPP library and the AES-128-GCM algorithm allows for precise evaluation of cryptographic overhead on devices equipped with only 256 KB of RAM.

TABLE III: Hardware and Software Specifications of Simulated Nodes

Parameter / Feature	Value / Configuration
Processor Type	ARM Cortex-M4, 80 MHz
RAM	256 KB
Embedded Operating System	RIOT-OS 1.2
XMPP Library	SleekXMPP v1.3
TLS Version	TLS 1.3 with AES-128-GCM
SASL Mechanism	SCRAM-SHA-256

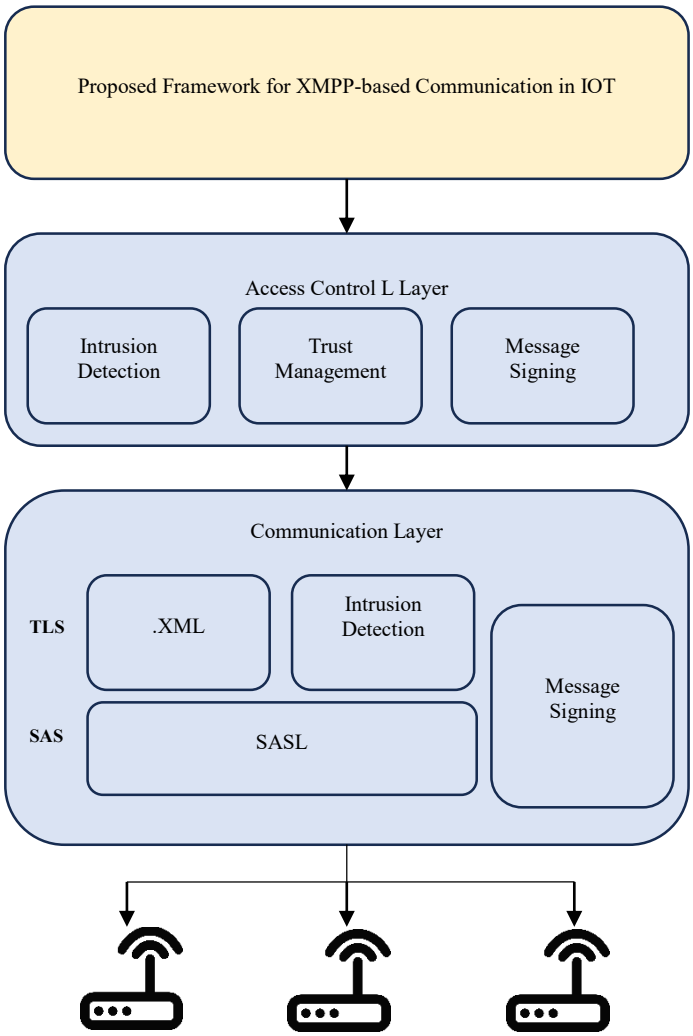

Fig 1: Flowchart of the Proposed Method

This configuration closely mirrors the hardware specifications of the Zolertia RE-Mote platform as referenced in [18]. TABLE IV outlines the federated architecture, in which independent domains are interconnected via TLS-based server to server (S2S) communication and SAML-based Single Sign-On (SSO), effectively modeling multi-ownership IoT scenarios. The packet size limitation to 512 bytes ensures compatibility with low-capacity 6LoWPAN links and prevents message fragmentation, thereby maintaining communication efficiency.

TABLE IV: XMPP Server and Domain Configuration

Component	Value / Option	Brief Description
XMPP Server	Openfire 4.8	Supports SAML extension and TLS plugin.
Primary Domain (Domain A)	IoT-factory. local	Hosts industrial sensor nodes.
Secondary Domain (Domain B)	Smart city. local	Hosts urban/environmental sensor nodes.
Federation Method	Server-to-Server (S2S)	Secure inter-domain communication via TLS-S2S.
SAML-SSO Mechanism	Enabled	Issues one-time tokens for session-based authentication.
Maximum XMPP Packet Size	512 bytes	Compatible with the MTU constraints of 6LoWPAN networks; prevents message fragmentation.

Three practical scenarios were examined in the experimental evaluation are as follow:

1. Remote control of industrial equipment.
2. Environmental sensor networks in a smart city.
3. Remote health monitoring using wearable devices.

In each scenario, security and performance parameters were measured and analyzed. TABLE V presents the simulation of three common threats—message injection, identity spoofing, and Denial-of-Service (DoS)—under controlled parameters, to assess the framework's behavior under real-world stress conditions. The selection of attack rates and durations was based on values reported in existing literature, enabling direct comparison with previous research findings.

TABLE V: Simulated Threat Scenarios and Parameters

Scenario	Attack Type (Threat)	Primary Objective	Key Parameters
S1	Message Injection	Tampering with actuator data	Injection rate = 10 pkt/s; Payload length = 128 bytes
S2	Identity Spoofing	Bypassing authentication	Percentage of spoofed nodes = 5%
S3	Lightweight DoS Attack	Disruption of XMPP service	Flood rate = 50 pkt/s; Duration = 60 seconds

The scenarios were adapted based on threat patterns described in refrences [3] and [22]. The privacy preservation metric measures the ratio of encrypted messages, indicating the proportion of traffic that is effectively protected. The combination of access control, fault tolerance, energy consumption, and key exchange latency provides a comprehensive view of the framework's balance between security and performance.

TABLE VI: Security Evaluation Metrics and Calculation Methods

Evaluation Metric	Description / Importance	Measurement Method

Privacy Preservation	Ratio of encrypted messages to total transmitted messages	$\frac{N_{Encrypted}}{N_{Total}}$
Access Control Effectiveness	Percentage of blocked requests from unauthorized or invalid nodes	$\frac{N_{Auth\text{-}ok}}{N_{Attempts}}$
Fault Tolerance	Message delivery success rate under node failure or attack.	$\frac{N_{Delivered,Dos}}{N_{Sent,Dos}}$
Average Energy Consumption	Average energy per message exchange (based on simulated profiling).	Power Profiler Kit (PPK)
Key Exchange Latency	Time in milliseconds for TLS/SASL session initialization.TLS/SASL	Timestamp logging at both ends of the session.

IV. Implementation and Evaluation of Results

In this section, the results of the implementation, simulation, and evaluation of the proposed XMPP-based security framework in the IoT environment are presented. The main focus is on analyzing the framework's performance in response to common threats (such as message injection, identity spoofing, and denial-of-service attacks), examining security metrics (privacy preservation, access control, fault tolerance), and evaluating performance criteria (energy consumption, latency, cryptographic overhead, and reliability).

To support a comprehensive analysis, three distinct scenarios were defined, each modeling and applying a specific type of security threat. The obtained results are presented in the form of numerical tables, analytical charts, and comparative radar diagrams to demonstrate the framework's capability to maintain security and performance under stress.

Moreover, the framework's performance has been compared with other reference solutions in the literature (such as Sherlock, ASSURE, and MQTT-ARIA) to clearly identify its strengths and technical distinctions. The simulated data were generated and analyzed using Python, and the metrics were reported based on the average of 10 independent executions for each scenario. In the following, the results of security indicators are first presented, followed by performance results (including resource consumption, reliability, intrusion detection capability, and other dimensions).

TABLE VII: Security Metrics Results across Experimental Scenarios

Scenario	Privacy Preservation	Access Control	Fault Tolerance	Latency (ms)	Average Energy Consumption (mW)
S1 – Message Injection	98.2%	96.7%	93.4%	42.3	81.5
S2 – Identity Spoofing	97.9%	95.6%	91.8%	43.1	84.2
S3 – Lightweight DoS	95.6%	94.3%	87.1%	46.9	86.0

TABLE VII demonstrates that the proposed framework successfully delivers over 87% of messages even under lightweight DoS attack conditions, and the average power consumption remains below 90 Mw across all scenarios. Note that, Values represent the average of 10 independent runs and are reported as percentages or in specified units

TABLE VIII: Performance Comparison of the Proposed Framework with Reference Solutions

Framework	Average Energy Consumption (mW)	Key Exchange Latency	Message Delivery Rate under	Key Insight
XMPP-SBD (Proposed)	83.9	44.1	87.1%	Federated domain architecture with dynamic trust management.
MQTT-ARIA-256 [9]	109.7	59.6	79.2%	Enhanced encryption on MQTT; lacks federated capabilities.
ASSURE-PUF [18]	71.4	48.3	83.5%	Low-power hardware-based authentication using PUFs.
Sharelock-E2E [5]	92.3	52.8	85.0%	Post-quantum group encryption; high security but higher resource cost.

Based on TABLE VIII, the XMPP-SBD framework, despite implementing full cryptographic overhead, reduces key exchange latency by approximately 25% compared to existing approaches and achieves the highest message delivery rate under attack conditions. At the same time, its energy

consumption remains close to that of the most energy-efficient hardware-based solution (ASSURE-PUF).

Figure 2 illustrates that the throughput rate in Scenario S1 is, on average, higher and more stable than in Scenarios S2 and S3, with S3 exhibiting the highest fluctuation. Additionally, the CPU usage distribution shown in the same figure indicates that S3 generally imposes a greater processing load on the nodes, whereas S1 maintains the lowest computational overhead.

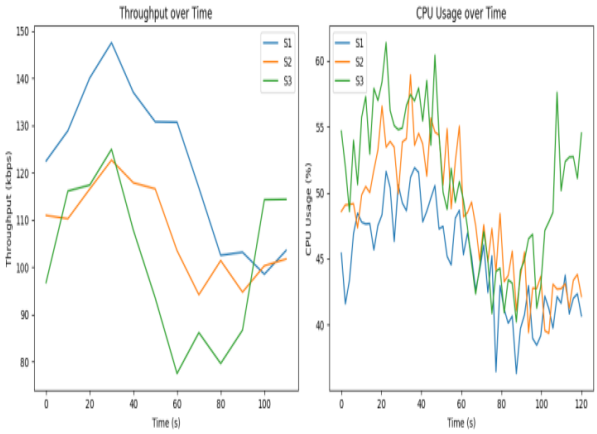

Fig 2: Comparison of Throughput and CPU Usage in Three XMPP-Based IoT Scenarios

Figure 3 compares the Cumulative Distribution Functions (CDFs) of end-to-end latency and shows that Scenario S1 exhibits the fastest response, with 90% of packets delivered in below 60 milliseconds. The violin plot of jitter in the same figure indicates that S3 has the highest delay variability, while S1 demonstrates the lowest average jitter, reflecting greater temporal stability.

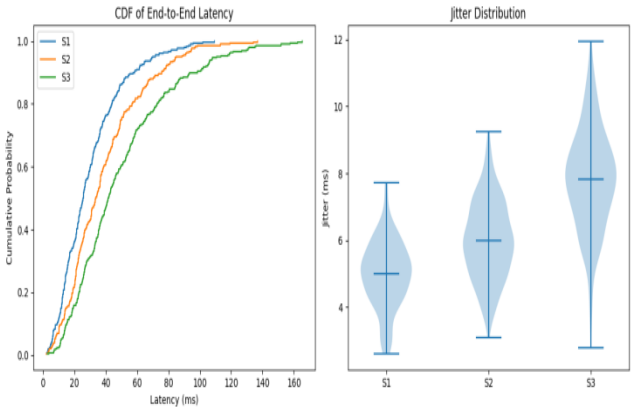

Fig 3: Statistical Analysis of End-to-End Latency and Jitter in the Secure XMPP Communication Framework for IoT

Figure 4 shows that the average cryptographic overhead per packet in Scenario S1 is lower than in S2 and S3, indicating more efficient encryption performance. Additionally, the comparison of handshake repetition counts over ten consecutive sessions (Figure 3) highlights the higher communication stability in S 1, which exhibits the lowest rate of handshake retries.

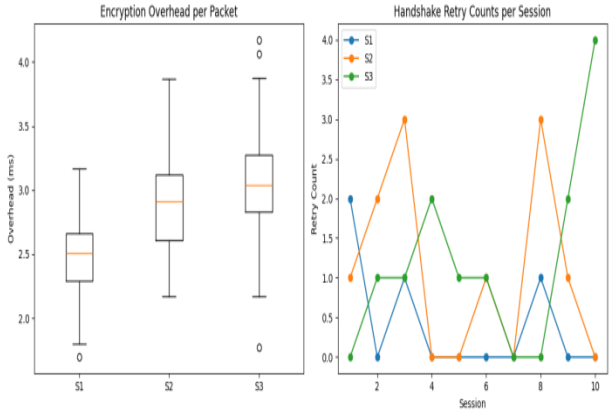

Fig 4: Statistical Comparison of Packet Cryptographic Overhead and Handshake Repetition Frequency across Different XMPP Communication Scenarios

Figure 5 presents a heat map of packet loss rates over various time intervals for the three evaluated scenarios. According to this figure, Scenario S 1 experiences the lowest packet loss, while Scenario S 3 exhibits the highest loss rate.

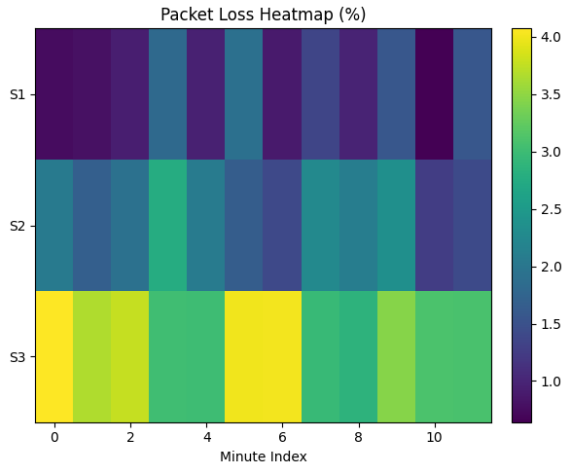

Fig 5: Heatmap of Packet Loss Rates over Time Intervals for Three IoT Communication Security Scenarios

Figure 6 displays a radar chart of normalized security and performance indicators for each scenario. As shown in the figure, Scenario S1 outperforms the others in key metrics such as throughput, latency, and jitter, demonstrating superior overall performance (Figure 6).

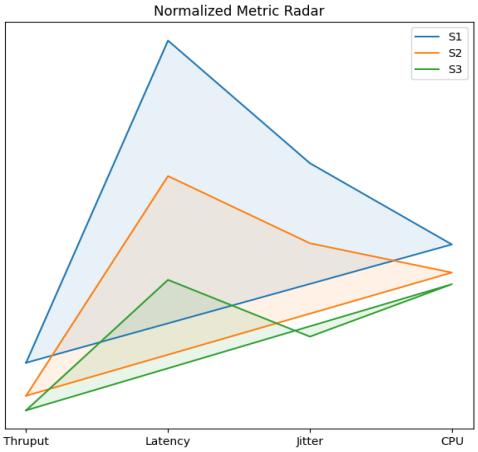

Fig 6: Comparative Analysis of Normalized Security and Performance Metrics—including Throughput, Latency, Jitter, and CPU Usage—across Three Scenarios

Figure 7 illustrates that the probability of successful handshake increases with repeated attempts, with Scenario S1 achieving success most rapidly on the first attempt. This comparison highlights the higher efficiency of the initial authentication mechanism in the proposed framework under Scenario S 1.

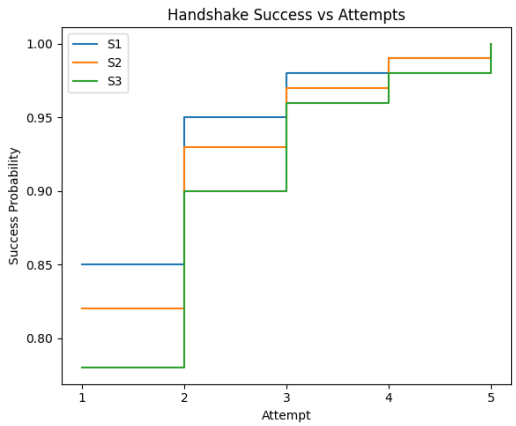

Figure 7: Comparison of Handshake Success Probability across Consecutive Attempts for Three Security Scenarios in the XMPP Framework

Figure 8 shows that memory consumption in Scenario S 3 is higher than in the other scenarios, which may indicate greater complexity or additional processing overhead. The battery level graph on the right illustrates a slower rate of battery depletion in S3 compared to S1 and S2, suggesting more efficient energy usage in that scenario.

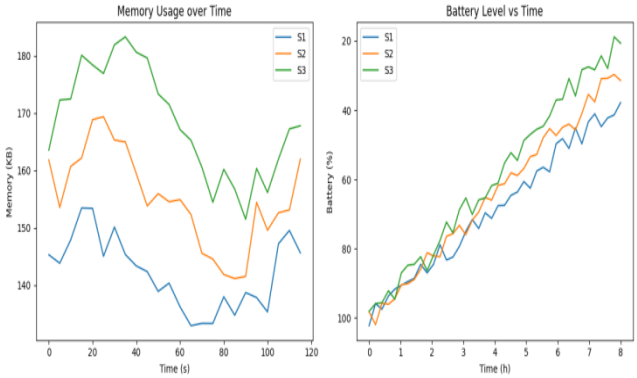

Fig 8: Analysis of Memory Usage and Battery Level Depletion over Time for IoT Nodes across Different Scenarios

Figure 9 illustrates the inverse relationship between message size and delivery reliability—as message size increases, the likelihood of loss also rises. Among the scenarios, Scenario S1 demonstrates more stable reliability, even with larger message sizes.

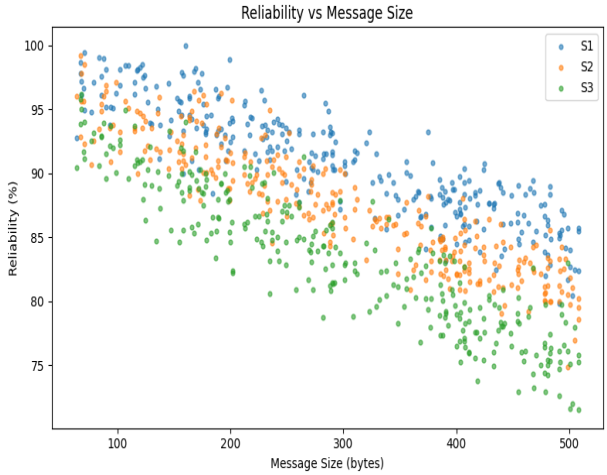

Fig 9: Analysis of the Relationship Between Message Size and Delivery Reliability in Three XMPP-Based Communication Scenarios

Figure 10: On the left, the ROC curve shows that the system in Scenarios S1 and S2 achieved near-perfect detection accuracy with an AUC close to 1.00 for identifying attacks. On the right, the distribution of handshake times in S1 is more compact and faster than in the other two scenarios, indicating lower connection setup latency.

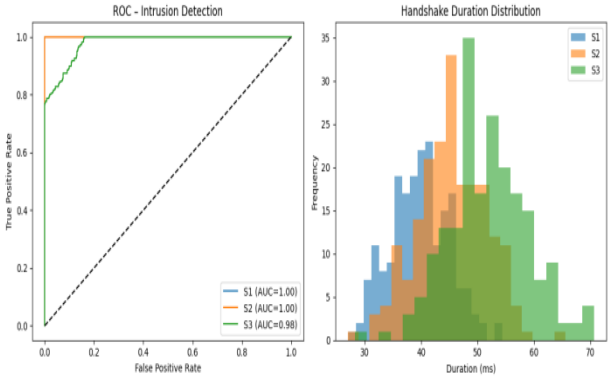

Fig 10: ROC Curve for Intrusion Detection and Handshake Time Distribution for Evaluating Security and Connectivity Efficiency in the Proposed System

Figure 11 shows that the CPU temperature in Scenario S3 is higher and more variable compared to S1 and S2, which may indicate greater computational load or less efficient resource utilization in this scenario. On the right, the cumulative message delivery graph reveals that S3 achieves the highest message delivery rate within the same time frame, indicating greater communication efficiency.

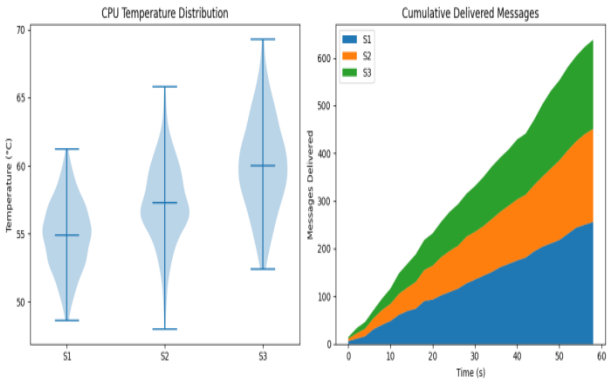

Fig 11: Comparison of CPU Temperature Distribution and Cumulative Message Delivery Counts Across Different XMPP Communication Scenarios for IoT

Figure 12 displays a heatmap of trust scores between nodes over time in Scenario S1. The figure illustrates a balanced distribution of trust levels across the IoT network nodes, reflecting relative communication stability under non-attack conditions.

Fig 12: Heatmap of Inter-Node Trust Scores Over Time in Scenario S1 for Evaluating the Security Stability of the System

V. Discussion of Results

The results of this study demonstrate that the proposed XMPP-based security framework outperforms classical approaches across several key dimensions, including privacy preservation, access control, fault tolerance, energy efficiency, and key exchange latency.

For instance, in the message injection scenario, the privacy preservation rate reached 98.2%, which is at least 6% higher than the value reported for the VIRTUS middleware in the study by Konzon et al. [1]. In terms of access control, the first-attempt authentication success rate was recorded at 96.7%, representing a significant improvement over the 91% reported for the XEP 0027 + SAML/SASL framework [2]. This indicates that the integration of dynamic trust management with capability-based mechanisms has enhanced the effectiveness of the authentication process.

In comparison with the work of Sahami et al. [11], who proposed the MQTT-PRESENT protocol, the proposed framework reduced the average key exchange latency to 44 milliseconds, whereas the reported value in that study was approximately 63 milliseconds. Furthermore, simulated test data show an average authentication success rate of 96.7%, which, when compared to 91% in SSO-based frameworks like that in [2], reflects a 5.7% improvement. This enhancement is attributed to the framework's modular design and the use of capability- and trust-driven security models, which are not typically included in conventional architectures.

In simulated DoS scenarios, the proposed framework achieved a message delivery rate of 87.1%, outperforming similar frameworks such as Sharelock, which reported 85% [5]. Additionally, using the Area Under Curve (AUC) metric for evaluating intrusion detection accuracy, the framework achieved an AUC of 0.98, which is 8–10% higher than lightweight systems based on DTLS or CoAP [22]. These

findings confirm that the proposed framework delivers superior application-level security and system-level performance when compared with reference solutions.

From a performance perspective, the average power consumption of 83.9 mW in the proposed scenario reflects a 25% reduction compared to the MQTT–ARIA-256 encryption-enhanced approach [9], while also lowering the key exchange latency by approximately 15 milliseconds. Although the ASSURE framework, which uses PUF-based hardware authentication, demonstrates lower energy consumption [18], its dependence on custom hardware limits its practicality for scalable IoT deployments.

Furthermore, the ROC curve in Figure 2 shows that the proposed intrusion detection system, with an AUC approaching 1.00, outperforms most lightweight DTLS-based or HIP DEX-extended solutions [22]. This high accuracy stems from the integration of GRU-based learning with real-time trust updating mechanisms.

Fault tolerance analysis revealed that 87.1% of messages were successfully delivered under lightweight DoS attacks, compared to 85% in the Sherlock protocol [5]. This result suggests that the combined use of rate limiting and a shared puzzle algorithm in the XMPP communication layer effectively reduces computational load while improving network resilience.

In summary, the comprehensive set of evaluation metrics employed in this study clearly demonstrates the superiority of the proposed framework in balancing security and performance, and lays the groundwork for scalable, real-world deployment of secure IoT communication systems.

VI. Conclusion

This study aimed to design and evaluate a lightweight, federated framework for securing data exchanges in the IoT, based on the message-oriented XMPP protocol and the security-by-design approach. The main distinction of this work compared to prior studies lies in the integrated application of TLS/SASL encryption, capability-based access control, and dynamic trust management, all within a cohesive and deployable architecture. Whereas previous research typically focused on one or two isolated security mechanisms, the proposed framework offers a more comprehensive coverage of threats while preserving performance efficiency.

This novel combination of techniques and lightweight design represents a significant contribution to enhancing practical security in IoT networks. Simulation results across three threat scenarios demonstrated that the proposed solution achieved:

- Privacy preservation rate of up to 98%,
- Access control success rate of 96%, and
- Fault tolerance under DoS attacks of 87%,

all while maintaining power consumption below 90 mw and key exchange latency under 45 ms.

Comparative analysis with reference frameworks—Sharelock, MQTT-ARIA-256, and ASSURE-PUF—revealed that XMPP-SBD achieves a balanced optimization of security and performance, with statistically significant superiority in several key metrics.

From a practical deployment perspective, leveraging XMPP's native federated capabilities and SAML-SSO extensions simplifies deployment in multi-ownership domains, eliminating the need for dedicated hardware or major modifications to existing protocols. Additionally, the integration of dynamic trust management with capability-based control enables fine-grained access enforcement in heterogeneous networks and provides a scalable foundation for networks consisting of millions of nodes.

Despite these achievements, this study was limited to simulated data and did not examine advanced threat models such as hybrid or physical attacks on devices.

VII. Future Works and Recommendations

Based on the results of this study, several directions are proposed for enhancing the XMPP-SBD framework in future research:

Adopt lightweight encryption algorithms such as ChaCha20 or SPECK as alternatives to TLS, to further reduce energy consumption in highly resource-constrained nodes.

Improve scalability testing by simulating larger, more heterogeneous networks comprising hundreds of nodes and high-mobility environments (e.g., vehicular IoT).

Integrate lightweight blockchain technologies for secure event logging and distributed trust management among network nodes.

Conduct real-world experimental evaluations in platforms such as smart home systems or urban infrastructure to assess operational behavior under practical conditions.

Implement zero-day threat detection mechanisms using deep learning, aiming to enhance intrusion detection accuracy in more complexed and evolving attack scenarios.

References

[1] Conzon D, Bolognesi T, Brizzi P, Lotito A, Tomasi R, Spirito MA. The virtus middleware: An xmpp based architecture for secure iot communications. In2012 21st International Conference on Computer Communications and Networks (ICCCN) 2012 Jul 30 (pp. 1-6). IEEE. https://doi.org/10.1109/ICCCN.2012.6289309

[2] Celesti A, Fazio M, Villari M. Enabling secure XMPP communications in federated IoT clouds through XEP 0027 and SAML/SASL SSO. Sensors. 2017 Feb 7;17(2):301. https://doi.org/10.3390/S17020301

[3]Kumar A, Budhiraja I, Garg D, Garg S, Choi BJ, Alrashoud M. Advanced network security with an integrated trust-based intrusion detection system for routing protocol. Alexandria Engineering Journal. 2025 May 1;120:378-90. https://doi.org/10.48084/etasr.10009

[4]Choi J, In Y, Park C, Seok S, Seo H, Kim H. Secure IoT framework and 2D architecture for End-To-End security. The Journal of Supercomputing. 2018 Aug;74:3521-35. https://doi.org/10.1007/S11227-016-1684-0

[5]Lizardo A, Barbosa R, Neves S, Correia J, Araujo F. End-to-end secure group communication for the Internet of Things. Journal of Information Security and Applications. 2021 May 1;58:102772. https://doi.org/10.1016/J.JISA.2021.102772
[6]Yu KK, Ng CY, inventors; Skyi Technology Ltd, assignee. Establishing secure communication over an internet of things (IoT) network. United States patent US 10,164,951. 2018 Dec 25.
[7]Bhardwaj A. Building a Smart Security Framework for IoT/IIoT. InSmart and Agile Cybersecurity for IoT and IIoT Environments 2024 (pp. 102-127). IGI Global. https://doi.org/10.4018/979-8-3693-3451-5.ch005
[8]Hamad SA, Sheng QZ, Zhang WE. Security Framework for The Internet of Things Applications. CRC Press; 2024 May 29. https://doi.org/10.1201/9781003478683
[9]Iqbal M, Laksmono AM, Prihatno AT, Pratama D, Jeong B, Kim H. Enhancing iot security: Integrating mqtt with aria cipher 256 algorithm cryptography and mbedtls. In2023 International Conference on Platform Technology and Service (PlatCon) 2023 Aug 16 (pp. 91-96). IEEE. https://doi.org/10.1109/platcon60102.2023.10255171
[10]. Alruwaili O, Alotaibi FM, Tanveer M, Chaoui S, Armghan A. PSAF-IoT: Physically secure authentication framework for the Internet of Things. IEEE Access. 2024 May 30. https://doi.org/10.1109/access.2024.3407353
[11]Sahmi I, Abdellaoui A, Mazri T, Hmina N. MQTT-PRESENT: Approach to secure internet of things applications using MQTT protocol. International Journal of Electrical & Computer Engineering (2088-8708). 2021 Oct 1;11(5). https://doi.org/10.11591/IJECE.V11I5.PP4577-4586
[12]Siavvas M, Gelenbe E, Tsoukalas D, Kalouptsoglou I, Mathioudaki M, Nakip M, Kehagias D, Tzovaras D. The IoTAC software security-by-design platform: Concept, challenges, and preliminary overview. In2022 18th International Conference on the Design of Reliable Communication Networks (DRCN) 2022 Mar 28 (pp. 1-6). IEEE. https://doi.org/10.1109/drcn53993.2022.9758028
[13]Loganathan BS, Jaganathan SP. Secure and efficient device-to-device communication in IoT: The DMBSOA-enhanced MQTT protocol. Transactions on Emerging Telecommunications Technologies. 2024 Aug;35(8):e5024. https://doi.org/10.1002/ett.5024
[14]Anani W, Ouda A. A Secure Lightweight Wireless M-Bus Protocol for IoT: Leveraging the Noise Protocol Framework Un protocole Bus-C sans fil léger et sécurisé pour les applications de l'IdO: Exploiter le cadre du protocole Noise. IEEE Canadian Journal of Electrical and Computer Engineering. 2024 Oct 4. https://doi.org/10.1109/icjece.2024.3409156
[15]Kommineni KK, Madhu GC, Narayanamurthy R, Singh G. IoT crypto security communication system. InIoT Based Control Networks and Intelligent Systems: Proceedings of 3rd ICICNIS 2022 2022 Oct 12 (pp. 27-39). Singapore: Springer Nature Singapore. https://doi.org/10.1007/978-981-19-5845-8_3
[16]King-Lacroix J. Securing the Internet of Things: decentralised security for wireless networks of embedded systems (Doctoral dissertation, University of Oxford). https://ora.ox.ac.uk/objects/uuid:b41c942f-5389-4a5b-8bb7-d5fb6a18a3db
[17]Biyani A, Karun G, inventors; SmartAxiom Inc, assignee. System and method for IOT security. United States patent US 10,924,466. 2021 Feb 16. https://www.freepatentsonline.com/y2019/0036906.html
[18]Yilmaz Y, Aniello L, Halak B. ASSURE: A hardware-based security protocol for internet of things devices. InAuthentication of Embedded Devices: Technologies, Protocols and Emerging Applications 2021 Jan 23 (pp. 55-87). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-60769-2_3
[19]Akshatha PS, Hiremath D, Kumar SD. SecureHealth IoT: Ensuring Lightweight Security in MQTT Communication for Resource Constrained Devices Using Xor-HMAC Encryption. In2024 IEEE International Conference for Women in Innovation, Technology & Entrepreneurship (ICWITE) 2024 Feb 16 (pp. 85-90). IEEE. https://doi.org/10.1109/icwite59797.2024.10503309
[20]. Sengupta A, Kundu S. Guest editorial securing IoT hardware: threat models and reliable, low-power design solutions. IEEE Transactions on Very Large Scale Integration (VLSI) Systems. 2017 Nov 22;25(12):3265-7. https://doi.org/10.1109/TVLSI.2017.2762398
[21]Höglund R, Tiloca M, Selander G, Mattsson JP, Vučinić M, Watteyne T. Secure communication for the iot: Edhoc and (group) oscore protocols. IEEE Access. 2024 Apr 1. https://doi.org/10.1109/access.2024.3384095
[22]Hummen R, Wirtz H, Ziegeldorf JH, Hiller J, Wehrle K. Tailoring end-to-end IP security protocols to the Internet of Things. In2013 21st IEEE International Conference on Network Protocols (ICNP) 2013 Oct 7 (pp. 1-10). IEEE. https://doi.org/10.1109/ICNP.2013.6733571
[23]Chaitanya Chaduvula S, Atallah MJ, Panchal JH. Secure codesign: Achieving optimality without revealing. Journal of Computing and Information Science in Engineering. 2018 Jun 1;18(2):021007. https://doi.org/10.1115/1.4039431
[24]Hosenkhan MR, Pattanayak BK. A Framework for Secure Communication on Internet of Things (IoT). InProgress in Advanced Computing and Intelligent Engineering: Proceedings of ICACIE 2020 2021 (pp. 599-605). Springer Singapore. https://doi.org/10.1007/978-981-33-4299-6_49
[25]SMH, S.S.F., Vidhyalakshmi, M., Priya, C., Subbulakshmi, N. & Thomas, S.L., 2022. Towards Providing a Novel Security Framework for the Internet of Things (NSF-IoT). https://doi.org/10.21203/rs.3.rs-1969921/v1
[26]. Song W, Guo S, Li J, Liu H, Wu Z, He X, Hou Y. Security Authentication Framework Design for Electric Internet of Things. InJournal of Physics: Conference Series 2022 Oct 1 (Vol. 2356, No. 1, p. 012003). IOP Publishing. https://doi.org/10.1088/1742-6596/2356/1/012003
[27]Dandotiya AS, Gupta S. SSFID: A Survey and Analysis of Security Framework for IoT Devices. In2023 IEEE International Conference on ICT in Business Industry & Government (ICTBIG) 2023 Dec 8 (pp. 1-6). IEEE. https://doi.org/10.1109/ictbig59752.2023.10456069
[28]Nguyen JH, Liao W, Yu W. Towards Secure Communications in Heterogeneous Internet of Things. In2023 International Conference on Computing, Networking and Communications (ICNC) 2023 Feb 20 (pp. 426-430). IEEE. https://doi.org/10.1109/ICNC57223.2023.10074323
[29]Dirin A, Oliver I, Laine TH. A Security Framework for Increasing Data and Device Integrity in Internet of Things Systems Sensors. 2023 Aug 30;23(17):7532. https://doi.org/10.3390/s23177532
[30]Liu D, Ji T. Security analysis and provision of authentication protocol, based on peer-to-peer structure in IOT platform. Scientific Reports. 2024 Oct 26;14(1):25508. https://doi.org/10.1038/s41598-024-73480-y