International Journal of Basic and Applied Sciences, 14 (7) (2025) 204-212

International Journal of Basic and Applied Sciences

Website: www.sciencepubco.com/index.php/IJBAS
https://doi.org/10.14419/8jbh3a60
Research paper

Temporal Authentication Model for The Internet of Things Edge Devices for Sustainable User Privacy

Jenish. M. [1] *, K. Karuppasamy [2], T. Bhuvaneswari [3], L. Mohana Kannan [4], Deepika. K. [5], S. V. Lakshmi [6]

[1] Research Scholar, Department of Electronics and Communication Engineering, RVS College of Engineering and Technology, Coimbatore
[2] K. Karuppasamy, Professor and Head, Department of Computer Science and Engineering, RVS College of Engineering and Technology, Coimbatore
[3] Assistant Professor, Department of Electronics and Communication Engineering, Dr. N.G.P. Institute of Technology, Coimbatore
[4] Associate Professor, Department of Biomedical Engineering, Erode Sengunthar Engineering College, Thudupathi, Erode
[5] Assistant Professor, Department of ECE, Karpagam Academy of Higher Education (Deemed To Be University), Coimbatore
[6] Assistant Professor, Department of ECE, SNS College of Technology, Coimbatore
**Corresponding author E-mail: jenesh.m@gmail.com*

Received: June 17, 2025, Accepted: October 15, 2025, Published: November 6, 2025

Abstract

Internet of Things (IoT) integrated edge devices are used in different real-time applications for providing cloud-based services to the users. As security issues are open in such integrated device platforms, the need for device authentication and user privacy is mandatory. This article, therefore, introduces a Temporal Authentication Model (TAM) for IoT-edge devices to sustain user privacy demands. The proposed model employs distributed federated learning to validate authentication and revocation processes under different sharing intervals. A temporal factor is used to validate the authentication sustainability without key changes across the sharing intervals. This temporal factor is used to decide the authentication or revocation for different devices. The distributed federated learning verifies the balance between these two processes to ensure maximum authentication. Thus, the proposed TAM improves the authentication rate by 11.39% and reduces the revocation failure by 11.39%, authentication time by 12.44%, and complexity by 11.61% for the operation time.

Keywords: *Device Authentication; Federated Learning; IoT-Edge; User Privacy.*

1. Introduction

Various information technologies are employed in textile industries, which elevates overall production and performance. Information technologies provide sufficient techniques and services to design the necessary platforms for improvement [1]. Emerging industrial technologies (EIT) are also implemented in textile industries, which reduces the challenging issues during manufacturing. EIT uses autonomous robots to design the products as per customers' preferences and tastes [2]. EIT maximizes the organization's sustainability, productivity, and impact on the industries. It also minimizes the energy consumption level during production, which leverages the efficiency and significance range of the textile industries [3]. An Industry 4.0-based decision-making model is used in the textile industry. The decision-making model employs a comprehensive analysis technique that analyzes the features and patterns of production services [4]. The analyzed features are used to improve the industry by implementing enormous techniques. A content analysis technique is also used to evaluate the factors that are required to enhance the development range of the industries [5].

Because changing environments make edge-based IoT systems need flexible authentication and responsive means of authentication. It generally happens that devices without real-time security adjustments keep changing from one network to another or innate from one role to another [1], [2]. The Adaptive Edge Security Framework creates dynamic security policies that automatically adjust themselves. The method observes the behavior, location, and activity pattern of the device in question. The framework enables seamless security while devices move or function differently [2], [3].

Typical techniques of authentication offer little assistance in resource-constrained environments with limited energy and memory. The constraints can harm performance by causing either slowdowns or battery drains or by erratic performance under high activity [4], [5]. The Secure and Efficient Lightweight Authentication Protocol (SELAP) offers a tiny solution for resource-constrained environments.

The approach employs small-sized message packets with a relatively weak encryption algorithm to verify the IoT devices' identity in almost real-time. SELAP saves processing time and energy by providing fast and secure access [5, 6].
Zero-trust model frameworks need more importance to deter attacks stemming from internal and external possible threats to the IoT systems. In these complex and distributed environments, static access control would not hold [7]. Under a Blockchain-Based Zero-Trust Authentication Scheme, default trust is completely ruled out, and each action of the device is verified [8]. The mechanism controls access through smart contracts by proof rather than location or identity labels. Each transaction is recorded on a blockchain ledger that cannot be tampered with or replayed. It ensures strong security and transparency in power-demanding edge networks [9, 10]. The article's contributions are:

1) The proposed description of a novel temporal authentication model for IoT-connected edge devices to maximize user privacy.
2) The incorporation of distributed federated learning ensures the allocation and revocation of the authentication process to maximize device-level security.
3) The presentation and discussion of performance metrics to verify the proposed model's efficiency using comparative analysis.

2. Related Works

Nakkar et al. [11] proposed a method for simplifying lightweight group authentication in edge computing. It enables asynchronous multi-user authentication in combination with a lightweight key-refreshing scheme. The method does not involve the redistribution of shares and also reduces the communication overhead. The method assures security through formal verification based on verification.
To guarantee mutual authentication plus forward secrecy in IoT systems, Seifelnasr et al. [12] designed the MAPFS protocol based on zero-knowledge proofs and random authentication requests. The technique distances the dependency on a central cloud administrator while implementing anonymous authentication. The method is based on the discrete logarithm and Diffie-Hellman assumptions for security assurance. The method also shows low computation, storage, and communication overhead on the Raspberry Pi 4.
Alruwaili et al. [13] developed a method called RAAF-MEC, which is the union of ECC, PUFs, hashing, and GIFT-COFB encryption. The method can dynamically derive keys to thwart storage-based attacks and insider threats. The method provides single sign-on while guaranteeing the freshness of the session. The method greatly reduces both communication and computation costs.
Tanveer et al. [14] presented the RAM-MEN scheme, which relies on cryptography and assumes the use of PU functions. The method secures the devices from insider threats and fake access points. Key agreements are scalable and secure with the method, and these agreements are formally validated. The method performs very well in reducing communication and computational overheads.
Zhang et al. [15] presented an innovative scheme for blockchain-based authentication that uses partial private keys. The method delegates trust to several blockchains to mitigate centralized points of failure. The method further enhances the integrity of identity and security of communication for IoT devices. The method is capable of resisting known attacks while being scalable and low in overhead.
For narrowband IoT environments, Zhao et al. [16] proposed a lightweight mechanism supported by LCHAOSAES encryption and edge-layer assistance for group authentication. The biased method decentralizes the load, hence reducing the load on the server. The method prevents identity leakage issues and promotes low-latency communication. The technique facilitates safe group verification while lowering signaling overhead.
Maiti et al. [17] developed a multiprocessor reporter-verifier architecture using known signature validation. The method enforces integrity verification by a hardware approach to curb internal threats. The model performs periodic firmware checks without adversely affecting device performance or power consumption. The method eliminates the dangers posed by malicious firmware from distrusted vendors.
Zhang et al. [18] designed stateless mutual authentication protocols. The method supports 5G-enabled low-latency networks with fast handover capability. The process reduces bandwidth requirements by minimizing the transmission of data and simply executing two signaling exchanges. The method significantly reduces edge-user authentication time compared to traditional protocols.
To support authentication better in edge-controlled industrial IoT systems, Shang et al. [19] have proposed a lightweight authentication scheme based on hash and XOR operations. The technique allows secure key agreement and anonymous mutual authentication. The method requires low-cost implementations in industrial ECS environments. The scheme possesses all the formal security strength and is a highly workable option.
Al-Shatari et al. [20] designed an architecture built around the LED cipher and PHOTON hash. The method concatenates ciphering and hashing so that hardware duplication is minimized. The method lowers the resource requirements in terms of logic area and power. The design is optimized for very constrained edge devices having FPGA implementations.
For developing a quantum-resistant decentralized authentication protocol, Shahidinejad et al. [21] proposed a lattice-based D2D authentication scheme in an edge and blockchain. The approach eliminates dependence on conventional cryptographies and supports key revocation over the blockchain. The method reduces the processing on the devices' sides and enhances overall security. The method withstands quantum and classical assaults with very strong security validation.
Cunha et al. [22] developed a technique based on physical unclonable functions, quantum key distribution, and blockchain. The approach can be used for tamper-proof device verification with low computational cost. The method ensures formats of decentralized transparency based on blockchain integrity-checking schemes. The approach has been validated using the Real-Or-Random model and the Scyther tool for robustness testing.
Liu et al. [23] designed an improved privacy-preserving scheme for IoT. An asynchronous federated learning (AFL) algorithm is utilized in the scheme to tackle the issues while providing privacy measures to the network. The scheme ensures the safety and privacy of the user's confidential data. The scheme reduces the loss of the aggregation rate of information. The designed scheme improves the accuracy of the privacy-preserving process.
Zhang et al. [24] proposed a lattice-based puncturable ciphertext policy attribute-based encryption (CP-ABE) method for cloud-assisted IoT. The private keys are analyzed and evaluated to identify the confidential data from the dataset. The identified data are secured from third-party attacks, which improves the flexibility of the network. The proposed method enlarges the security and privacy ratio of the networks.
Li et al. [25] developed an accurate and efficient privacy protection FL (AEPPFL) model for IIoT. The model encrypts the channels and sensitive data in the network. The model evaluates the necessary parameters for training, which are encrypted for further processing. It also minimizes the compactional cost and latency rate of the process. The developed model achieves high precision in protecting sensitive data from attacks.

Wang et al. [26] introduced a preventive audit for data sharing for power IoTs. The explicit details of the information are analyzed to prevent data leakage. The model is used to avoid unwanted risks during data sharing services. The model uses a probability exchange to provide preventive audits for the confidential data. The introduced model enlarges the effectiveness of the system.
Islam et al. [27] proposed an optimized privacy-utility tradeoff framework for blockchain-based IoT. The proposed framework uses a heuristic search algorithm (HSA) to reduce the computational complexity of the network. The framework evaluates the real-world datasets of the owners to understand the transparency. Experimental results show that the proposed framework optimizes the unwanted issues in the networks.
The authentication for edge devices in IoT is a temporal process, i.e., it relies on the connectivity between the devices and the authentication type for sustainability. Time-dependent changes in key generation and utilization are mandatory to retain authentication and user privacy. The above-discussed methods rely on direct and blockchain-based security measures to ensure IoT-edge devices are operational with user privacy preservation. However, the change in any security parameter from the device or user results in privacy failures. Besides, the unattended revocation results in privacy breaches as the chances of key reuse without the service provider's knowledge are high. Considering these problems for administering user privacy, this article proposes a time-dependent authentication model with temporal factor validation. The proposed model is different from the existing methods by computing the temporal factor based on device authentication and user privacy balance on multiple request processing and sharing intervals.

3. Proposed Temporal Authentication Model

In the growing Internet of Things (IoT) edge devices industry, it is important to maintain secure communication with user privacy. The edge devices typically deal with sensitive information, which renders them easy targets for attacks by malicious parties. Device authentication is incorporated to create trust among devices and users. The use of temporal aspects like operation time during the authentication process allows for dynamic and context-dependent security mechanisms. The timely revocation of compromised or outdated devices is necessary for the integrity of the IoT ecosystem. The proposed model's process is illustrated in Fig. 1.

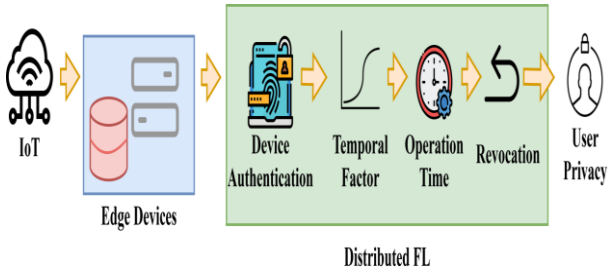

Fig. 1: Proposed TA Model Illustration.

To reinforce user privacy, a distributed federated learning framework is included. This enables real-time validation of operation time and revocation decisions without exposing raw data. This approach offers a decentralized privacy-preserving solution to IoT device authentication. The IoT edge device behavior is analyzed as E_{IoT} In the following equation, to ensure user privacy.

$$E_{IoT} = (Sn_{data} + Cmp_{load}) + G_{consum}(t) + (t_{change} + N_{inter}) + Sy_{error} \quad (1)$$

The sensor data is denoted as Sn_{data} Captured from device sensors to form the raw input for decision-making, and the computational load required to process the data is represented as Cmp_{load} To monitor the impact on device performance. The resource consumption is associated with both data processing and communication at a time. (t) is denoted as G_{consum}. The change in operational time is expressed as t_{change} Helps to check device behavior and varying security conditions. The number of interactions made by the device with other nodes is represented as N_{inter} and Sy_{error} Denotes the system error. This enables real-time detection of anomalies during unauthorized usage in a complex IoT environment. For authentication, it is important to generate a key that is formulated as K_{gen} In the following equation, ensure that only trusted devices participate in the network.

$$K_{gen} = (U_{IoT} \times t_{operate}) + N_{inter} + E_{IoT} + K_{user} \quad (2)$$

The unique IoT device identifier for authentication is denoted as U_{IoT} and $t_{operate}$ Represents the operating time during key generation, which measures the uniqueness of the key during communication between devices. The key generated from the user side is denoted as K_{user} It is obtained to match the server key to minimize denied key access. The authentication is considered valid during $K_{gen} = K_{user}$ To monitor whether the generated key matches the user key. It helps to analyze the replication of keys and ensure that the generated key cannot be reused to reduce the risk of attacks. This refines the process of key generation for successful authentication during communication between IoT devices. Device authentication is computed as D_{auth}The equation below verifies the identity and operational process of the network after successful key generation.

$$\left.\begin{aligned} D_{auth} = (K_{gen} \times t_{operate}) + K_{re-gen} \times (t_{rec} + K_{user}) \\ \text{where} \\ D_{auth} = 1 \rightarrow \text{if } K_{gen} = K_{re-gen} \text{ and } |t_{operate} - t_{rec}| \leq \omega \end{aligned}\right\} \quad (3)$$

The en of $(K_{gen} \times t_{operate})$verifies the key generation at the device side to ensure that the key is unique to the equest. The regeeratedkey is denoted asK_{re-gen} and the time at which the request is received is repnted as t_{rec} in $K_{re-gen} \times (t_{rec} + K_{user})$ analyze the expected time to regenerate the key according to a user request. The device is accepted only during $D_{auth} = 1$ by comparing $K_{gen} = K_{re-gen}$ and $|t_{operate} - t_{rec}| \leq \omega$ with the thresholdvalue ω. If valuelue exceeds the limit as $K_{gen} = K_{re-gen}$ and $|t_{operate} - t_{rec}| > \omega$, then the device is rejected from the server to safeguard the data from eternal attacks. This maintains the integrity of the device to preserve

user privacy. The temporal factors were determined as Y_{fact} in the following equation to identify the factors that are relevant to IoT edge devices.

$$Y_{fact} = t_{operate} \times \left[1 \times \left(D_{auth} + t_{change}\right)\right] + \left(K_{gen} \times Cmp_{load}\right) \tag{4}$$

Here, t_{change} is used to update the time based on the device authentication to evaluate the temporal reliability between the devices. A high Y_{fact} value with $t_{change} \rightarrow \left|t_{operate} - t_{rec}\right| \forall D_{auth} = 1$ indicates the trustworthiness of the device based on recent authentication validation. This updated authentication change is fed into the system to make optimal revocation decisions. Operational time computes the expected behavior of the IoT edge device and monitors the usage patterns, which are derived in the equation below.

$$t_{operate} = \int_{t0}^{t} D_{status} + Y_{fact} + N_{inter} \times \left[K_{re-gen} \times t_{rec}\right] - D_{inative} \tag{5}$$

The operation activation time of the device between the initial time t0 and the current time t is to prioritize the recent operating device over the older device in the network. The device status is denoted as D_{status} that identifies the active state of the device when it is successfully authenticated with $D_{auth} = 1$ and free from security risks. The inactive state of the device is denoted as $D_{inative}$ which is analyzed during $D_{auth} = 0$ with $K_{gen} \neq K_{re-gen}$. This device status verification allows systems to distinguish between consistently active devices and those that have irregular behavior, which is important for optimal authentication and anomaly detection. The authentication process is illustrated in Fig. 2.

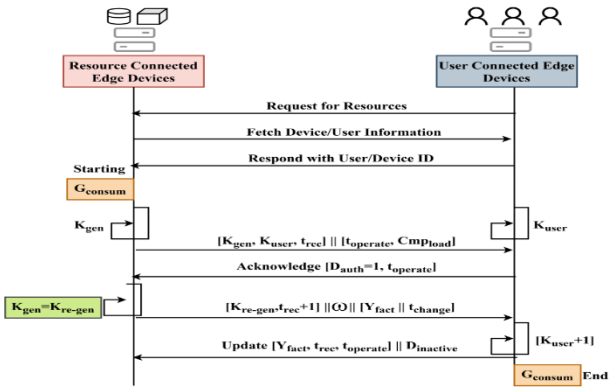

Fig. 2: Authentication Process between the Devices.

In Fig. 2, the authentication process between distinct edge devices is illustrated. The edge devices connected with the resources and users are verified for authentication. This D_{auth} is valid for $t_{operate}$ to retain user privacy through device authentication. The conventional device information is shared for G_{consum} initialization. The K_{gen} and K_{user} are congruently generated for authenticated $\forall\, D_{auth} = 1$ in t_{rec} response. If the $t_{change} > t_{rec}$ time, then the need for new authentication session is required. Based on the Y_{fact} observed from the previous interval, the K_{re-gen} is performed to serve the requests in $(t_{rec} + 1)$ interval. The $D_{auth} = 1$ is the valid condition for updating security demands across various communication demands. The $(K_{user} + 1)$ is the tallying factor for the acknowledged response interval to maximum ω in the authentication process. The device status is validated by the distributed federated learning, which is discussed below, to maintain higher user privacy in IoT networks.

3.1. Distributed federated learning (DFL)

Each edge device processes its operation data locally by including temporal aspects such as usage patterns and operation time. It learns the local behavior of the device from distributed sources to identify anomalies in device operation and outdated operation time without infringing on user data. The abnormal patterns over time are discovered to assist with the validation and revocation of devices. The revocation process is strongly triggered through smart local models and efficiently backed up by a strong federated consensus. DFL maintains privacy by providing user-specific data and reducing communication overhead with high scalability. It also adapts to changes in device behavior over time to improve authentication with a privacy-preserving method of authenticating IoT devices within a dynamic environment. The process of DFL is expressed as L_{DFL} in the following equation.

$$\left.\begin{aligned} D_{status} = D_{auth}(t0 - t) + \left[t_{operate} - D_{inative}(t0 - t)\right] \\ N_{inter}(t0 - t) = D_{auth} - D_{inative} \\ L_{DFL} = D_{status} + N_{inter}(t0 - t)\ \forall D_{auth} = 1 \rightarrow \text{validate} \end{aligned}\right\} \tag{6}$$

The device status is verified by monitoring its authentication and inactive condition from the initial time to the current time. The node interaction N_{inter} is verified by evaluating the difference between $(t0 - t)$ to determine the actual device state without operational duration. This process $L_{DFL} \forall D_{auth} = 1 \rightarrow \text{validate}$ enables secure and privacy-preserving validation of IoT device behaviors. If the validation passes, the system can trust the authentication and process anomaly detection and revocation to improve privacy. If the validation fails, the system re-trains the device for accurate anomaly detection. This distributed learning enhances the security and decision-making across the IoT network. From this validation, the system performs revocation and is formulated as D_{revoc} in the equation below.

$$\left.\begin{aligned} D_{revoc} = t_{change} + Anm_{detect} + (1 - B_{trust}) - L_{DFL} \\ \text{where} \\ D_{revoc} = (B_{trust} + D_{auth}) \geq \omega \\ B_{trust} \rightarrow 0 \leq B_{trust} \leq 1 \end{aligned}\right\} \tag{7}$$

The anomaly detection score is denoted as Anm_{detect} and the authentication trust value is represented as B_{trust} to monitor how the device eliminates anomalous and unauthorized behavior from the system. It verifies multiple behavioral and temporal factors within the trust level range $0 \leq B_{trust} \leq 1$ to enable precise device revocation decisions. The system performs revocation only when the device satisfies $D_{revoc} = (B_{trust} + D_{auth}) \geq \omega$ and the revocation probability is high. B_{trust} The value is close to zero. This improves the overall capacity of the system to protect user privacy with an accurate device revocation decision. The DFL process for revocation is presented in Fig. 3.

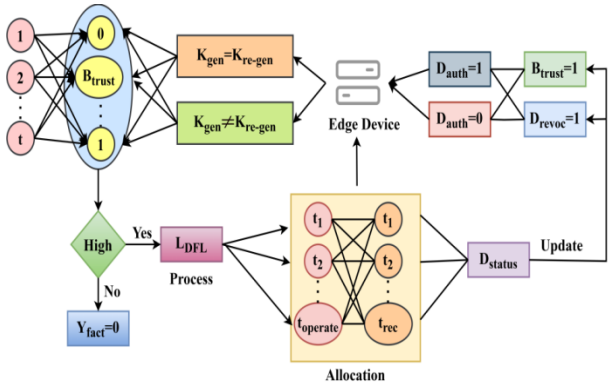

Fig. 3: DFL Process for Revocation.

The DFL process is depicted in Fig. 3 for consecutive $t \forall B_{trust}$ estimated. The two cases of $(K_{gen} = K_{re-gen})$ and $(K_{gen} \neq K_{re-gen})$ are validated to detect Y_{fact}. The $Y_{fact} = 1$ is the maximum L_{DFL} process for allocating requests under $t_{operate}$ such that t_{rec} is served. The allocation is preceded using D_{status} update. This update is either a revocation or a trust update; if the revocation is true, then $D_{auth} = 0$ and therefore sharing is paused. If the $B_{trust} = 1$, then $D_{auth} = 1$ such that the generated key is pursued for further authentication, else a new key is generated. Therefore, the L_{DFL} the process is repeated until the maximum operation time is served. Using different L_{DFL} iterations, the t_{rec} is sustained for the revocation interval until D_{status} is retained. The user's privacy is preserved as $U_{privacy}$ in the following equation, when the affected device authentication is revoked.

$$U_{privacy} = \max_{B_{trust}} \left[D_{auth} + L_{DFL} + D_{revoc} + Y_{fact} + t_{operate} \times \left(\frac{1}{B_{trust}} \right) \right] \quad (8)$$

The authentication trust value is maximized with device authentication to obtain high and secure user privacy in an IoT environment. The computation of $U_{privacy} \propto \left(\frac{1}{B_{trust}} \right)$ is incorporated to reduce the low authentication trust that affects the privacy level of the user data. The sum of $L_{DFL} + D_{revoc}$ monitors the privacy validation when the user-linked devices are unreliable and are not revoked properly, with a high impact on privacy leakage. This helps to protect user data through validation and revocation when the device is directly affected by threats. Continuous monitoring of device behavior and a timely revocation process preserve the device from external threats and safeguard user privacy in IoT devices.

3.2. Self-analysis

In the self-analysis section, the temporal factor and user privacy level factors are described with graphical illustrations. The authentication and user privacy levels are analyzed in this self-analysis section. These two factors are considered as the impact and target (objective) for the proposed method in temporal intervals. Based on $t_{operate}$, B_{trust}, Y_{fact}, and L_{DFL}The above parameters are illustrated in Figs. 4 and 5.

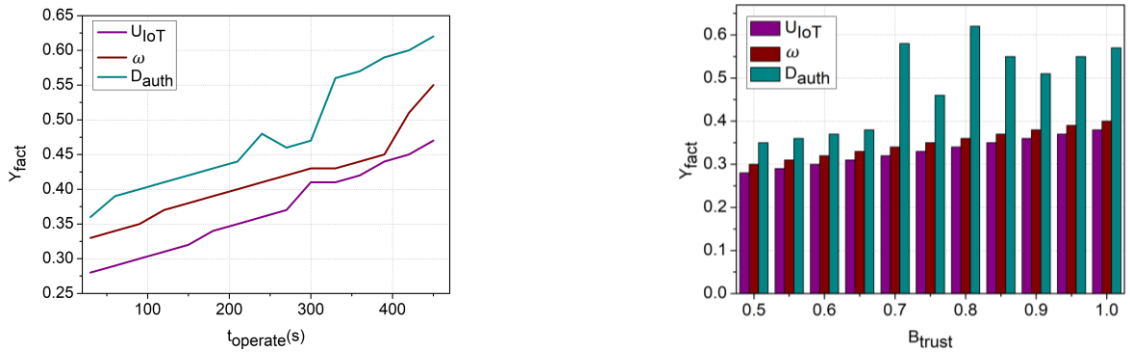

Fig. 4: Temporal Factor Analysis.

The temporal factor was improved consistently over time based on their performance, which is more stable when compared to the other method. The existing method relied on static time sessions, which failed to detect subtle time-based anomalies and resulted in high false positives. The proposed method continuously assesses the operational time changes within particular intervals to monitor the authentication of actively participating devices. This allows for more accurate authentication and a timely revocation process for handling time-sensitive security issues (Fig. 4).

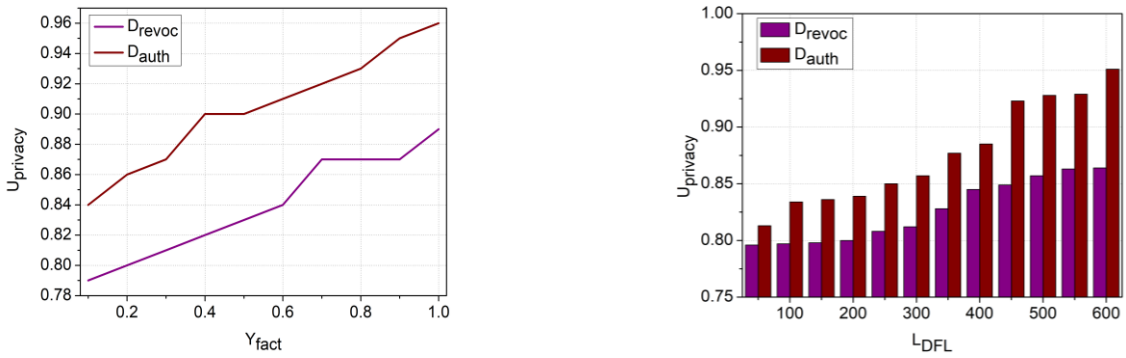

Fig. 5: Privacy Level Analysis.

The incorporation of federated learning keeps user data localized and avoids raw data transmission to central servers to achieve high user privacy levels when compared to the existing methods. Some existing methods lack distributed intelligence and adaptive protection mechanisms, which leads to a lower privacy level when facing similar threats. Trust-based authentication with periodic revocation in the proposed method minimizes the risk of data exposure from untrustworthy devices. The proposed method maintains a consistently higher privacy score in scenarios involving multiple devices with sensitive user data (Fig. 5).

4. Results and Discussion

The proposed model is analyzed using Contiki Cooja-based simulation to verify its output and performance. The network is modeled with 60 edge devices capable of operating between 30s and 450s for a maximum of 50 requests. In the authentication process, elliptic curve cryptography with a 160-bit key is used. The maximum validity time is 240s, and therefore, for a complete 450s interval, requires 2 K_{re-gen} instances. The revocation time is between 3s and 5s for any number of $D_{auth} = 0$ users. Using a single cloud server device, 200 users are connected to serve the request with authentication.

4.1. Case study and analysis

In the case study analysis section, we describe the performance of the proposed model in coherence with the dataset provided in [28]. In this dataset, a real-time assessment of IoT connected to a local network infrastructure is considered. The purpose is to access different resources through remote access for surveillance devices. In this experimental setup, distributed denial of service and spoofing adversaries are accounted for. DDoS restricts the communication links between the devices/ resources and the external controller. Spoofing adversary replicates the service provider's address to represent false data or/ resource. These two adversaries are identified by analysing the variations in flow time, flow rate, acknowledge count, synchronization count, request, and responses. This analysis is distinguishable for both the adversary models considered. The flow time, rate, and acknowledge count are evaluated for DDoS, and the rest for the spoofing adversary. For the application of TAM, B_{trust} and the authentication rate is also analysed for both adversaries. This analysis is presented in Table 1.

Table 1: Analysis of Authentication Parameters

Network Parameter	B_{trust}			Authentication Rate		
	Devices=20 DDoS	Devices=40	Devices=60	Devices=20	Devices=40	Devices=60
Flow Time (ms)	532.06	2247.25	2741.25	0.9508	0.9430	0.9553
Flow Rate	0.98-0.89	high		0.9565	0.9472	0.9449
Synchronization Count	19	36	52	0.9495	0.9587	0.9437
Acknowledge Count	16	28	49	0.9309	0.9332	0.9304
Request	70	130	220	0.9248	0.9270	0.9451
Responses	65	123	216	0.9108	0.9183	0.9103
Spoofing						
Flow Time (ms)	632.06	854.36	2837.19	0.9570	0.9426	0.9513
Flow Rate	0.895	0.921	0.978	0.9544	0.9234	0.9436
Synchronization Count	18	32	58	0.9539	0.9357	0.9481
Acknowledge Count	85	135	255	0.9515	0.9492	0.9475
Request	81	132	247	0.9361	0.9164	0.9392
Responses	73	122	245	0.9204	0.9208	0.9200

Each edge device manages its operational data on-site by incorporating temporal aspects such as usage trends and the duration of operations. It learns the local behavior of the device from distributed sources to detect anomalies in device functionality and outdated operational times without compromising user data. Over time, abnormal patterns are identified to support the validation and revocation of devices. The revocation process is robustly initiated through intelligent local models and effectively supported by a strong federated consensus. The device's status is confirmed by monitoring its authentication and inactivity from the beginning to the present. If validation is successful, the system can rely on the authentication and proceed with anomaly detection and revocation to enhance privacy. If validation is unsuccessful, the system re-trains the device for precise anomaly detection. This distributed learning strengthens security and decision-making throughout the IoT network. The TAM's influence on the aforementioned adversaries is analysed using Y_{fact} and $U_{privacy}$ achieved. Depending on the $t_{operate}$ and L_{DFL} the authentication stability is analysed. The impact of the above-mentioned scenario is considered with the conventional TAM processes (Table 1).

4.2. Comparative analysis

The proposed TAM is validated using different metrics: authentication rate, renovation failure, authentication time, and complexity. The methods LCHAOSAES [16] and RAAF-MEC [13] are used along with the proposed model to verify its efficiency.

4.3. Authentication rate

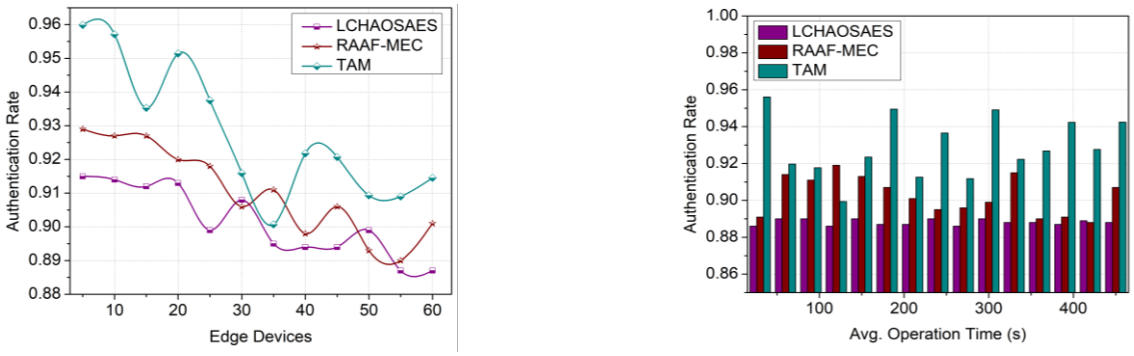

Fig. 6: Authentication Rate.

The proportion of successful authentications over total authentication attempts is high in the proposed method. Temporal factor verification and distributed model validation with $L_{DFL} = D_{status} + N_{inter}(t0 - t)\ \forall D_{auth} = 1 \rightarrow$ validate ensuring only genuine devices are actively synchronized within the system. The number of interactions verification enhances the accuracy of the system to adapt to varying operational times without compromising user privacy. Key generation based on operational time ensures that only devices with precise data are authenticated for IoT operations. High authentication rates reduce downtime and enhance system responsiveness with increased user satisfaction for secure IoT edge devices (Fig. 6).

4.4. Revocation failure

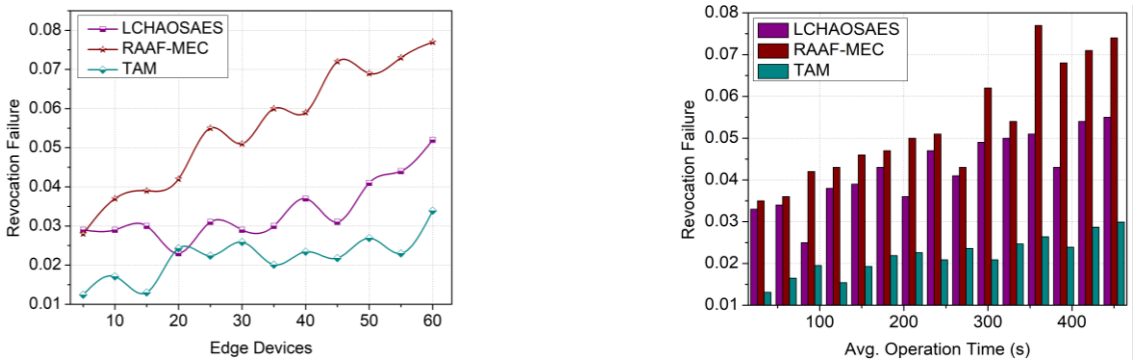

Fig. 7: Revocation Failure.

A low revocation rate by the proposed method ensures that the system correctly identifies and eliminates compromised or anomalous devices in the IoT environment. This is achieved by evaluating the revocation score based on $D_{revoc} = (B_{trust} + D_{auth}) \geq \omega$ to aggregate temporal drift, degradation, and anomaly during privacy detection. Continuous device monitoring for revocation improves threat detection and isolates malfunctioning devices. This low revocation maintains user privacy and network integrity to prevent the devices from malicious behavior that remains undetected (Fig. 7).

4.5. Authentication time

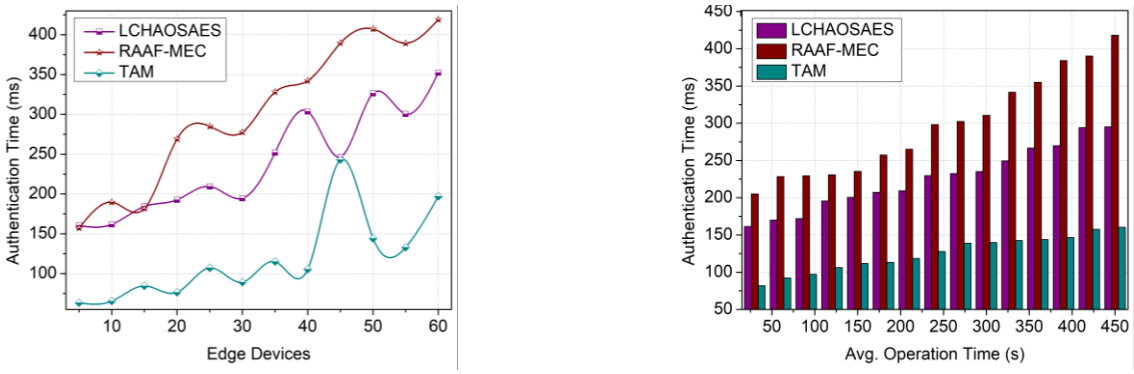

Fig. 8: Authentication Time.

The time taken by the system to authenticate for privacy is less in the proposed method, which indicates faster detection processes. Reduced authentication time is achieved by implementing edge-based key matching and device authentication to make a distributed deci-

sion to avoid delays during computations. The proces of $D_{auth} = (K_{gen} \times t_{operate}) + K_{re-gen} \times (t_{rec} + K_{user}) = 1$ states that the device is completely authenticated and no raw data is transmitted with latency, which disrupts operations and lowers the user experience. It minimizes communication overhead and speeds up the authentication in real-world IoT systems (Fig. 8).

4.6. Authentication complexity

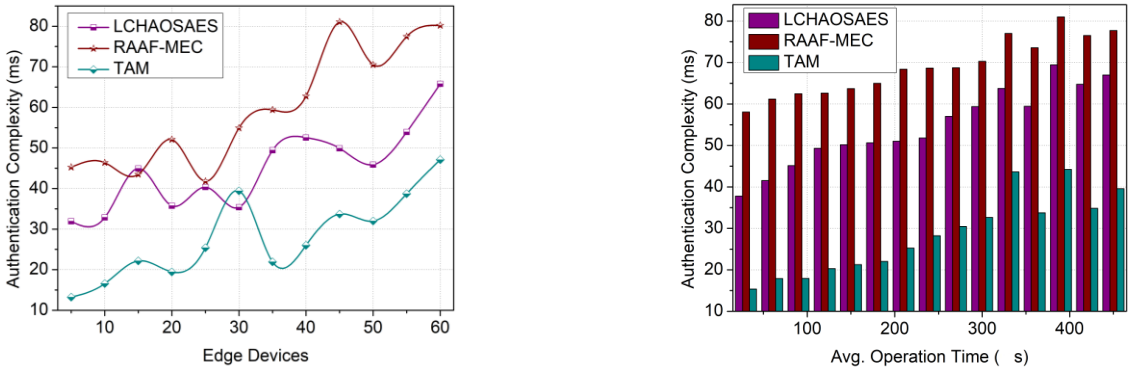

Fig. 9: Authentication Complexity.

The computational complexity of authentication remains low in the proposed method based on the increased intelligence of distributed federated learning. The computation of $K_{gen} = (U_{IoT} \times t_{operate}) + N_{inter} + E_{IoT} + K_{user}$ helps the system to integrate edge-device-based key generation by comparing it with operational time using simple federated updates. It limits feature dimensions used in federated learning and avoids frequent model retraining to manage system updates. This keeps accurate authentication in resource-constrained IoT edge devices with minimum complexity to ensure better efficiency and longer device lifespans (Fig. 9). Tables 2 and 3 present the comparative analysis results for the maximum edge devices and average operation time.

Table 2: Comparative Analysis Results for Maximum Edge Devices

Metrics	LCHAOSAES	RAAF-MEC	TAM
Authentication Rate	0.887	0.91	0.9561
Revocation Failure	0.052	0.077	0.0339
Authentication Time (ms)	352.32	412.04	196.977
Authentication Complexity (ms)	65.77	80.18	47.108

The proposed TAM improves the authentication rate by 11.52% and reduces the revocation failure by 11.86%, authentication time by 12.11%, and complexity by 11.82% for the maximum edge devices.

Table 3: Comparative Analysis Results for Average Operation Time

Metrics	LCHAOSAES	RAAF-MEC	TAM
Authentication Rate	0.888	0.907	0.9424
Revocation Failure	0.055	0.074	0.0299
Authentication Time (ms)	295.19	418.25	160.345
Authentication Complexity (ms)	67	77.71	39.58

The proposed TAM improves the authentication rate by 11.39% and reduces the revocation failure by 11.39%, authentication time by 12.44%, and complexity by 11.61% for the operation time.

4.7. Scalability analysis

Following the comparative analysis, the scalability limits of the proposed model are described. Apart from the devices considered in the comparative analysis, for scalability assessment, the device count is varied from 50 to 600. This variation is studied for network latency and authentication rate under different conditions Y_{rates}. The rate of change of Y_{rate} influences the latency and authentication rate that is tabulated in Table 4.

The latency and authentication rate vary with the device count; the interaction design and modification require a trust factor with authentication. Verifying the frequency of interactions leverages the system's ability to adjust to different operational durations without compromising user privacy. By creating keys that depend on operational time, only devices with accurate data are authorized to perform IoT tasks. High authentication rates minimize downtime and enhance system responsiveness, resulting in greater user satisfaction with secure IoT edge devices. The proposed method shortens the time required for the system to authenticate privacy, indicating quicker detection processes. This reduction in authentication time is accomplished by utilizing edge-based key matching and device authentication, which allows for a distributed and device-adaptable decision-making process to prevent delays during computations (Table 2).

5. Conclusion

Secure and privacy-oriented IoT device authentication needs a multi-aspect solution that considers temporal dynamics and operational integrity. To serve this concept, this article proposed the temporal authentication model. Through the incorporation of operation time and device revocation into the authentication process, the system only allows valid and timely devices to engage in the network. Distributed federated learning enhances privacy by allowing collaborative model training without centralizing sensitive information. This strengthens user privacy and reinforces the overall security infrastructure of IoT edge environments for more secure and reliable IoT deployments. Thus, the proposed model is reliable in achieving an 11.52% high authentication rate and reducing authentication complexity by 11.82% for the maximum edge devices.

References

[1] Halgamuge, M. N., & Niyato, D. (2025). Adaptive edge security framework for dynamic IoT security policies in diverse environments. *Computers & Security*, 148, 104128. https://doi.org/10.1016/j.cose.2024.104128.

[2] Pawlicki, M., Pawlicka, A., Kozik, R., & Choraś, M. (2023). The survey and meta-analysis of the attacks, transgressions, countermeasures and security aspects common to the Cloud, Edge and IoT. *Neurocomputing*, 551, 126533. https://doi.org/10.1016/j.neucom.2023.126533.

[3] Javadi, A., Sadeghi, S., Pahlevani, P., Bagheri, N., Rostampour, S., & Bendavid, Y. (2025). Secure and Efficient Lightweight Authentication Protocol (SELAP) for multi-sector IoT applications. *Internet of Things*, 101499. https://doi.org/10.1016/j.iot.2025.101499.

[4] Li, S., Zhang, H., Shi, H., Ma, M., & Wang, C. (2024). A novel blockchain-enabled zero-trust-based authentication scheme in power IoT environments. *The Journal of Supercomputing*, 80(14), 20682-20714. https://doi.org/10.1007/s11227-024-06262-y.

[5] Khan, M., Hatami, M., Zhao, W., & Chen, Y. (2024). A novel trusted hardware-based scalable security framework for IoT edge devices. *Discover Internet of Things*, 4(1), 4. https://doi.org/10.1007/s43926-024-00056-7.

[6] Liu, M., Lu, N., Wen, Y., Cheng, Q., & Shi, W. (2023). Sea: Secure and efficient public auditing for edge-assisted IoT aggregated data sharing. *Mobile Networks and Applications*, 1-12. https://doi.org/10.1007/s11036-023-02146-2.

[7] Zhonghua, C., Goyal, S. B., & Rajawat, A. S. (2024). Smart contracts attribute-based access control model for security & privacy of IoT system using blockchain and edge computing. *The Journal of Supercomputing*, 80(2), 1396-1425. https://doi.org/10.1007/s11227-023-05517-4.

[8] Jiang, N., Zhai, Y., Wang, Y., Yin, X., Yang, S., & Xu, P. (2024). Location Privacy Protection for the Internet of Things with Edge Computing Based on Clustering K-Anonymity. *Sensors (Basel, Switzerland)*, 24(18), 6153. https://doi.org/10.3390/s24186153.

[9] Chen, Z., Deng, Y., Yang, M., Wu, X., Wang, X., & Wei, P. (2025). Privacy-Preserving Dynamic Spatial Keyword Query Scheme with Multi-Attribute Cost Constraints in Cloud–Edge Collaboration. *Electronics,* 2079-9292, 14(5). https://doi.org/10.3390/electronics14050897.

[10] Wang, J., & Li, J. (2024). Blockchain and access control encryption-empowered IoT knowledge sharing for cloud-edge orchestrated personalized privacy-preserving federated learning. *Applied Sciences*, 14(5), 1743. https://doi.org/10.3390/app14051743.

[11] Nakkar, M., AlTawy, R., & Youssef, A. (2022). GASE: A lightweight group authentication scheme with key agreement for edge computing applications. *IEEE Internet of Things Journal*, 10(1), 840-854. https://doi.org/10.1109/JIOT.2022.3204335.

[12] Seifelnasr, M., AlTawy, R., Youssef, A., & Ghadafi, E. (2023). Privacy-Preserving Mutual Authentication Protocol with Forward Secrecy for IoT–Edge–Cloud. *IEEE Internet of Things Journal*, 11(5), 8105-8117. https://doi.org/10.1109/JIOT.2023.3318180.

[13] Alruwaili, O., Tanveer, M., Aldossari, S. A., Alanazi, S., & Armghan, A. (2025). RAAF-MEC: Reliable and anonymous authentication framework for IoT-enabled mobile edge computing environment. *Internet of Thing*s, 29, 101459. https://doi.org/10.1016/j.iot.2024.101459.

[14] Tanveer, M., & Aldossari, S. A. (2025). RAM-MEN: Robust authentication mechanism for IoT-enabled edge networks. *Alexandria Engineering Journal*, 112, 436-447. https://doi.org/10.1016/j.aej.2024.10.116.

[15] Zhang, S., & Cao, D. (2024). A blockchain-based provably secure anonymous authentication for edge computing-enabled IoT. *The Journal of Supercomputing*, 80(5), 6778-6808. https://doi.org/10.1007/s11227-023-05696-0.

[16] Zhao, G., Chen, H., & Wang, J. (2024). An edge-assisted group authentication scheme for the narrowband internet of things. *Complex & Intelligent Systems*, 10(5), 6597-6618. https://doi.org/10.1007/s40747-024-01514-z.

[17] Maiti, A., & Kist, A. A. (2025). A Zero-Trust Multi-Processor Reporter-Verifier Design of Edge Devices for Firmware Authenticity in Internet of Things and Blockchain Applications. *Journal of Sensor and Actuator Networks*, 14(2), 35. https://doi.org/10.3390/jsan14020035.

[18] Zhang, J., Ouda, A., & Abu-Rukba, R. (2024). Authentication and key agreement protocol in hybrid edge–fog–cloud computing enhanced by 5G networks. *Future Internet*, 16(6), 209. https://doi.org/10.3390/fi16060209.

[19] Shang, W., Wen, X., Chen, Z., Xiong, W., Chang, Z., & Cao, Z. (2024). Lightweight authentication scheme for edge control systems in Industrial Internet of Things. *Frontiers of Information Technology & Electronic Engineering*, 25(11), 1466-1478. https://doi.org/10.1631/FITEE.2400497.

[20] Al-Shatari, M., Hussin, F. A., Aziz, A. A., Eisa, T. A. E., & Tran, X. T. (2023). IoT Edge Device Security: An Efficient Lightweight Authenticated Encryption Scheme Based on LED and PHOTON. *Applied Sciences*, 13(18), 10345. https://doi.org/10.3390/app131810345.

[21] Shahidinejad, A., & Abawajy, J. (2023). Decentralized lattice-based device-to-device authentication for the edge-enabled IoT. *IEEE Systems Journal*, 17(4), 6623-6633. https://doi.org/10.1109/JSYST.2023.3319280.

[22] Cunha, T. B. D., Kiran, M., Ranjan, R., & Vasilakos, A. V. (2024). Physical unclonable functions and QKD-based authentication scheme for IoT devices using blockchain. *Internet of Things*, 28, 101404. https://doi.org/10.1016/j.iot.2024.101404.

[23] Liu, S., Zhu, L., Zhang, W., Miao, Y., Leng, T., & Choo, K. K. R. (2024). Accuracy-Improved Privacy-Preserving Asynchronous Federated Learning in IoT. *IEEE Internet of Things Journal*. https://doi.org/10.1016/j.iot.2024.101404.

[24] Zhang, T., Jiang, M., Luo, F., & Guo, Y. (2025). A lattice-based puncturable CP-ABE scheme with forward security for cloud-assisted IoT. *IEEE Internet of Things Journal*. https://doi.org/10.1109/JIOT.2025.3559567.

[25] Li, G., Lei, H., Liu, F., Li, L., & Jin, H. (2025). AEPPFL: Accurate and efficient privacy protection federal learning in industrial IoT. *IEEE Internet of things journal.* https://doi.org/10.1109/JIOT.2025.3562064.

[26] Wang, B., Wang, Y., Guo, Q., Lin, Y., & Yu, Y. (2024). Preventive audits for data applications before data sharing in the power IoT. *IEEE Internet of Things Journal.* https://doi.org/10.1109/JIOT.2024.3483929.

[27] Islam, M., Rehmani, M. H., Gao, L., & Chen, J. (2025). An optimized privacy-utility trade-off framework for differentially private data sharing in blockchain-based internet of things. *IEEE Internet of Things Journal.* https://doi.org/10.1109/JIOT.2025.3530247.

[28] https://www.unb.ca/cic/datasets/iotdataset-2023.html.