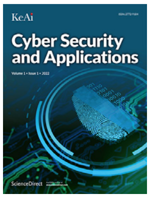
Contents lists available at ScienceDirect

Cyber Security and Applications

journal homepage: http://www.keaipublishing.com/en/journals/cyber-security-and-applications/



An efficient IoT group association and data sharing mechanism in edge computing paradigm

Haowen Tan*

Cyber Security Center, Kyushu University, Fukuoka 819-0395, Japan

ARTICLE INFO

Keywords:
Edge Computing
Wireless Communication
IoT
Security
Privacy-Preserving

ABSTRACT

Despite its benefits and promising future, security and privacy challenges for the IoT wireless communication of edge computing environment remain unaddressed. As a result, proper authentication mechanisms are critical, especially in the extreme scenario where some edge facilities are not functional. For the above consideration, in this paper we develop an efficient IoT group association and updating mechanism in edge computing paradigm. The proposed scheme can provide data transmission and communication guarantees for special practical scenarios. The group key updating process in our architecture only necessitates minor changes on the EI side, whereas the decryption information of some IoT devices remains constant if the devices have not been revoked. The proposed strategy can accomplish the desired security features, according to the security analysis.

1. Introduction

Because of the inherent open wireless communication features [1–3], IoT data sharing is vulnerable to a variety of security and privacy problems, particularly in IoT group communication environments with a large number of participating devices. Advanced security measures and privacy preservation mechanisms are critical for edge infrastructure in this circumstances [4,5]. Effective and efficient authentication mechanism between IoT terminal users (TUs) and the regarding edge infrastructure (EI) could provide preliminary protection for IoT data exchange. As a result, various known and unknown secure threats such as eavesdropping, impersonation, and the malicious replaying operations conducted by adversaries can be prevented, which is important for the current booming 5G industry and the future of 6G communications. Nowadays, because of the proliferation of edge computing techniques, the large storing and instant data processing requirements of IoT network can be satisfied with the cloud and edge infrastructure.

Meanwhile, the edge computing infrastructure is recognized as a decentralized computing architecture that shifts applications, corresponding data, and service processing from the network's central nodes to the network's logical terminal devices. Edge computing is capable of dividing large services that would otherwise be processed and managed totally by the central server or node into much smaller, more manageable chunks. In the next, it will distribute them to the edge devices for processing. As a matter of fact, the edge nodes are the local servers that are closer to the user-end devices, which can reduce latency and speed up data processing and delivery. Edge computing reduces latency, increases efficiency, and improves security and privacy protection by bringing intelligent analytical processing services closer to the data source. For example, in 2014, more than 30 percent of smart meters from Spain's three largest electricity service providers were found to have severe security vulnerabilities that could be exploited by attackers. Therefore, the attackers are able to commit electricity fraud or even manage the entire circuit systems. Security attacks have been even more damaging in the industrial IoT space, with the 2018 TSMC manufacturing site attack, the 2017 ransomware incident, and the 2015 Ukraine massive power outage all causing significant damage to targeted industrial IoT systems and individual devices.

As for the various types of applications and implementations in the scope of Internet of Things (IoT), the participating IoT devices will record/generate/transmit a large amount of data involving user privacy. Therefore, data security risks are becoming more serious. More than a million families and children's data, conversation recording data, and action track data have been leaked since 2015. Hundreds of thousands of users' credit card accounts, biometric data, and other personal information were stolen when a vending machine company in the United States was hacked in July 2017. Additionaly, a Chinese security firm that makes IoT cameras warns that hackers can use the commonly used default credentials to directly access the user devices and even acquire the sensitive cameras' live data, which leads to significant security danger to every customer.

Wireless IoT communication, as an important data transmission channel of IoT, has very limited energy, processing capacity, storage capacity and communication capacity. The overall security reliability of IoT is harmed by the fact that a large number of traditional devices lack synchronous configuration protection. Meanwhile, the convergence

* Corresponding author.
E-mail address: tan_halloween@foxmail.com

https://doi.org/10.1016/j.csa.2022.100003
Received 9 February 2022; Received in revised form 16 April 2022; Accepted 16 June 2022
Available online 5 July 2022

and diversification of IoT terminals and applications have increased the security risk associated with the IoT industry. Attackers have a large and extensive entry point for network attacks thanks to the growing variety of IoT interconnected devices, which has resulted in a slew of problems and challenges for IoT. In this case, edge computing technologies can be used to significantly improve the security level of IoT systems based on this, allowing users' private data to be protected during both the interaction and storage processes.

Many research accomplishments have been accomplished recently, focusing on the IoT safe authentication issue using edge computing, which employs a variety of cryptographic design and verification methodologies. It's worth noting that in some cases, the key generation center (KGC) arranges all of the keying information for specific IoT devices, potentially causing the key escrow problem. Therefore, it is critical for the IoT device to construct its own partial secret pair and then retain the key information hidden from all other entities, even the key generation center. By adopting the unique partial confidential secrets from both the KGC and the device itself, certificateless encryption outperforms other approaches in this regard. It's worth noting that neither the KGC nor the IoT device has access to the other party's partial secret.

We assume the particular IoT data sharing scenario intended for extreme environments, where the edge facilities may be disabled or compromised [6–8]. In fact, in most isolated natural landscapes, such as mountains, desert areas or tropical rain forests, especially in sparsely populated areas, it's possible that the edge infrastructures are not always available. That is, most of the IoT devices of this region that originally rely on the wireless communication for data sharing may be out of touch. In this case, we utilizes the nearby other IoT devices that are still in contact with the edge infrastructure to conduct the message forwarding service. In this case, even in out-of-service region, the IoT devices can still maintain instant data sharing with the remote cloud server. Meanwhile, all the nearby IoT devices are capable of constructing the randomized data forwarding and delivering networks if necessary.

2. Related work

Nowadays, the topics of data security and user privacy protection towards IoT environments are extensively investigated. Numerous studies regarding authenticated key management and reliable vehicular data exchange of different IoT sceanrios have been conducted so far. As for the vehicular communication, in 2012, Lu *et al.* [9] developed a dynamic key updating protocol DIKE to satisfy the privacy-preserving and reliability requirements of location-based VANET services (LBS). The distributed session keys are cooperatively updated by the involved devices whenever the revocation process initializes. In [10], the validating process towards certificate revocation lists (CRLs) in terms of vehicular message authentication is improved with the adopted hash chains. Subsequently, a scalable group key management scheme with message encryption is proposed by Aliev *et al.* [11]. Notably, the matrix-based encryption algorithm is utilized in the distributed architecture so that enhanced security characteristics and efficiency can be guaranteed. Similarly, Aman *et al.* [12] developed a robust IoV authentication scheme with unclonable functions. The approaching devices are verified by the gateway instead of each RSU. In 2021, Cai *et al.* [13] proposed a conditional privacy protection mechanism adopting ring signcryption and identity-based cryptosystem. Identities of the misbehaving nodes can be revealed with the assigned tracking marks. Recently, several authenticated key management (AKM) schemes are developed [14–16].

Specifically, identity-based and attributed-based cryptographic techniques have been widely adopted in the authenticated key management process. A cooperative message authentication and key management framework is developed in 2011 [17], where decentralized message verification tasks are allocated to each legitimate device. Meanwhile, with the aim to enhance the communication efficiency of emergency services, Yeh *et al.* [18] proposed an attributed-based access control scheme ABACS so that data confidentiality property is provided. Afterward, the pseudonymous authentication-based conditional privacy protocol PACP [19] is presented by Huang *et al.*. The improvement in terms of computation and storage cost during the message validation process is achieved. Thereafter, two privacy-preserving authentication mechanisms [20,21] for secure vehicular communication are respectively proposed in 2014. Subsequently, He *et al.* developed an identity-based VANET authentication method without pairing [22]. Accordingly, the computational complexity of the verification session can be significantly reduced. In 2020, Feng *et al.* applied the blockchain-assisted authentication framework in [23] for privacy preservation. Dynamic revocation and conditional tracking towards the misbehaving devices are enabled. Another attribute-based encryption (ABE) model [24] is developed in order to meet the responding time requirement of edge intelligence-empowered IoV. The proposed ABEM-POD adopts the parallel outsourced decryption process, which is of specific usage for the tree access structure. Another attribute-based verification scheme for secure data sharing is proposed in [25].

3. Preliminaries

In this part, the fundamental principles and preliminary knowledge are given so as to facilitate the reader's understandings.

3.1. Lagrange polynomial interpolation

Definition 1 (Degree of Polynomial over. $\mathbb{F}_p$**)** Let $\mathbb{F}_p$ be a finite field, $P(x) = \sum_{i=0}^{t} \epsilon_i x^i$ be a non-zero polynomial, where $\epsilon_t \neq 0$, the arbitrary positive integer t is defined as the degree of $P(x)$ such that $\deg P(x) = t$.

Accordingly, define $\{(x_0, y_0), \ldots, (x_j, y_j), \ldots, (x_k, y_k)\}$ as a set of $k+1$ distinctive data points such that $\forall m \neq j$, $x_m \neq x_j$. The polynomial $Q_k(x)$ of the degree k over the finite field $\mathbb{F}_p$ is built according to

$$Q_k(x) = \sum_{i=0}^{k} a_i x^i,$$

where $Q_k(x_i) = y_i$ for all $i = 0, \ldots, k$. The unique Lagrange basis polynomials $\ell_j(x)$ $(0 \leq j \leq k)$ of degree at most k are computed as

$$\begin{aligned} \ell_j(x) &= \frac{(x-x_0)}{(x_j-x_0)} \cdots \frac{(x-x_{j-1})}{(x_j-x_{j-1})} \frac{(x-x_{j+1})}{(x_j-x_{j+1})} \cdots \frac{(x-x_k)}{(x_j-x_k)} \\ &= \prod_{m=0,m\neq j}^{k} \frac{x-x_m}{x_j-x_m} \end{aligned}.$$

The corresponding interpolation polynomial $L_k(x)$ in the Lagrange form can be defined as $L_k(x) = \sum_{j=0}^{k} y_j \ell_j(x)$. That is,

$$L_k(x) = \sum_{j=0}^{k} \left(\prod_{m=0,m\neq j}^{k} \frac{x - x_m}{x_j - x_m} \right) y_j.$$

Accordingly, for $\forall i \neq j$,

$$\ell_j(x_i) = \prod_{m=0,m\neq j}^{k} \frac{x_i - x_m}{x_j - x_m} = 0,$$

and

$$\ell_j(x_j) = \prod_{m=0,m\neq j}^{k} \frac{x_j - x_m}{x_j - x_m} = 1$$

hold. Hence, the reconstruction of the polynomial $Q_k(x)$ can be performed with $k+1$ distinctive data points on the graph of polynomial $Q_k(x)$ and $L_k(x)$.

3.2. Bilinear pairing

Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be the cyclic additive group and multiplicative group generated with prime order q. The mapping $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ is defined as a bilinear pairing with the following characteristics:

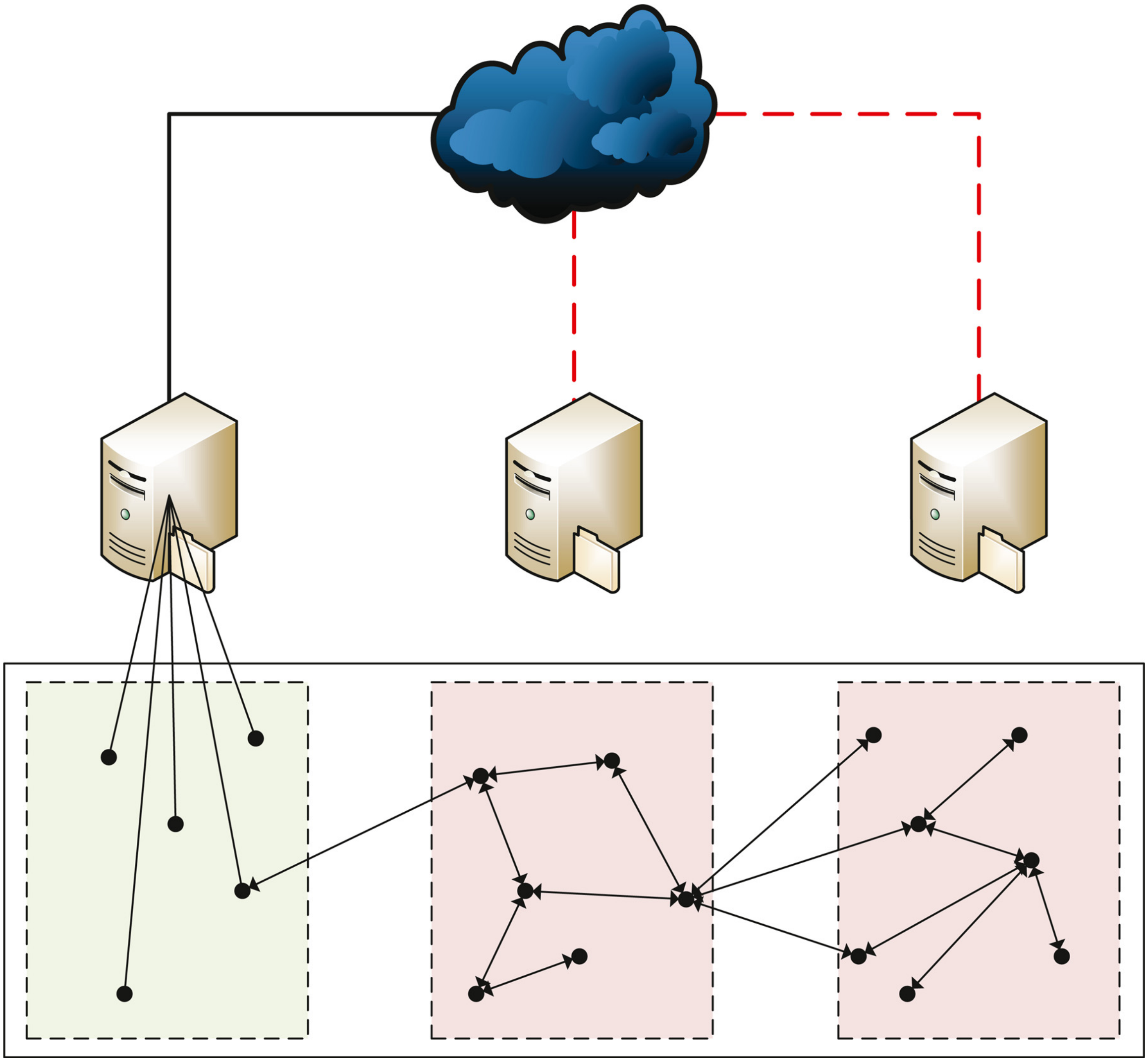


Fig. 1. System Model.

1. *Bilinearity:* $\forall P, Q, R \in \mathbb{G}_1$ and $\forall a, b \in \mathbb{Z}_q^*$, there is

$$\begin{cases} \hat{e}(aP, bQ) = \hat{e}(P, bQ)^a = \hat{e}(aP, Q)^b = \hat{e}(P, Q)^{ab} \\ \hat{e}(P, Q + R) = \hat{e}(Q + R, P) = \hat{e}(P, Q)\hat{e}(P, R) \end{cases}.$$

2. *Non-degeneracy:* $\exists P, Q \in \mathbb{G}_1$ such that $\hat{e}(P, Q) \neq 1_{\mathbb{G}_2}$, where $1_{\mathbb{G}_2}$ is the identity element of $\mathbb{G}_2$.
3. *Computability:* $\forall P, Q \in \mathbb{G}_1$, there is an efficient algorithm to calculate $\hat{e}(P, Q)$.

3.3. Security objectives

The objectives of our design are to enhance the vital security properties for edge computing scenarios. The following security requirements should be satisfied.

- *User Anonymity:* Normally, messages originated from the same TU carry identical or regular patterns, which is likely to expose the linkability. Hence, by analyzing large quantities of eavesdropped messages, the non-negligible details can be deduced, which seriously compromise the user privacy. Therefore, anonymous message delivery is utterly necessary for all the participating TUs.
- *Session Key Establishment:* The shared session keys between edge devices and the system should be established after mutual validation among the participating two or more parties, so that the further data exchange can be preserved with the shared keys.
- *Conditional Privacy-Preserving:* Conditional privacy-preserving is made up of two important privacy-related criteria: user privacy protection and TU identity retrieval. On the one hand, personal data about a user's genuine identity should be kept safe at all times in order to prevent malevolent activities like illegal tracing and eavesdropping on individual TUs. In emergency situations, however, the law enforcement agency (LEA) should be able to expose the true TU's identity. In other words, user privacy is presumed to be conditional on the detection and disclosure of compromised or disabled TUs.
- *Mutual Authentication:* Mutual authentication is the most basic but most important security feature of the edge environment, ensuring that all edge entities check each other before the data delivery session begins. The absence of mutual authentication before the communication process could result in serious security flaws.

3.4. System model

In our design, the entire edge infrastructure consists of the cloud server, the edge infrastructure (EI) and multiple terminal users (TUs). The utilized architecture of the proposed design is shown in Figure 1, which is considered as a specific edge communication scenario devoted to emergency situations [26].

In our design, the edge infrastructure (EI) is the essential part of the Internet of Things (IoT) system. EI is in charge of significant processes such as system setup, user registration, key management, and verification, among others. EI is assumed to be robust to all types of attacks and to remain authentic at all times in our design [27]. Because the role of EI is undertaken by commercial groups in the proposed plan, it cannot be entirely trusted. We regard the EI to be a trustworthy but suspicious authority, where all major generating and identification processes are carried out properly. Note that the EI only generates a portion of the private key for the registered TUs, while each TU is designed to produce the remaining portion of the private key on its own. In this method, the key escrow issue is avoided. EI, in particular, provides direct wireless connection for certified devices within its effective range, while devices outside of its coverage can obtain cellular connectivity indirectly [28–30].

The terminal users (TUs) are envisioned to be the IoT communication's terminal users. TUs are involved in data transmission that is routed over the EI framework in hostile environments. That is, the participating TUs not only deliver the messages they generate, but they also convey the routed data from other TUs. Even though some devices are outside of the EI coverage, a particular TU's interaction with surrounding devices ensures good connectivity to all remaining TUs. It's worth emphasizing that, for security reasons, the TUs should be verified before accessing the edge network [31–33].

4. Proposed scheme

The certificateless group authentication technique is provided in this paper with the goal of offering an enhanced authentication scheme for edge communication in an IoT paradigm. The proposed scheme is divided into two parts: certificateless authentication and group key distribution.

The approach of certificateless authentication and group key management is discussed, with a focus on verification for participating TUs. The registration, verification, and group key distribution are the three steps of our authentication design. As a result, the TU registration, as well as certain non-trivial key initialization preparation, takes place during the offline registration. It's worth noting that all TUs must register with EI before accessing the edge networks.

In the authentication step, major certificateless authentication solutions are presented. The group key is then generated and transmitted in a timely and trustworthy manner. Furthermore, the technique for group key update is introduced, allowing TUs to manage their membership quickly and efficiently. It's worth mentioning that our solution uses a certificateless encryption strategy for mutual verification between EI and TUs, which eliminates the need for key escrow. The goal of bilinear pairing is to provide increased security features. For practical circumstances in a complicated environment, the proposed certificateless authentication for edge communication is suitable.

The offline registration phase is intended for the initialization including the essential key information management, and TU registration. Initially, the bilinear group $(\mathtt{P}, \mathrm{G}, \mathrm{G}_{\mathrm{S}}, \hat{e})$ is defined, where $\mathtt{P}$ is a λ-bit prime, G and $\mathrm{G}_{\mathbb{S}}$ denote two multiplicative cyclic groups with the prime order $\mathtt{P}$. Hence the bilinear map $\hat{e}$ is constructed as $\hat{e} : \mathrm{G} \times \mathrm{G} \rightarrow \mathrm{G}_{\mathrm{S}}$. $g, w \in \mathrm{G}$ are the generators and $\mathfrak{I} \in \mathbb{Z}_{\mathtt{P}}$ is the randomly generated master key. At first, the unique license ID_i is assigned to each TU so that $ID_i \in \{0,1\}^*$ and $i \in [1,t]$, where t denotes the total number of the registered TUs. Hence the edge device set is defined as $S = \{ID_1, \dots, ID_t\}$. Moreover, the cryptographic hash functions $H_1 : \{0,1\}^* \rightarrow \mathrm{G}$, $H_2 : \mathrm{G} \times \mathrm{G} \times \mathrm{G}_{\mathrm{S}} \rightarrow \mathbb{Z}_{\mathtt{P}}$, $H_3 : \mathrm{G}_{\mathrm{S}} \times \mathrm{G}_{\mathrm{S}} \rightarrow \mathrm{G}_{\mathtt{P}}$ and $H_4 : \mathrm{G} \times \{0,1\}^* \rightarrow \mathbb{Z}_{\mathtt{P}}$ are defined. EI computes $\aleph_i = H_1(ID_i)$ for $ID_i \in S$, and then selects $\eth_i \in \mathrm{G}$ and $\varkappa_i \in \mathbb{Z}_{\mathtt{P}}$, with $i \in [1,t]$. EI computes:

$$\mathtt{A}_i = \eth_i \aleph_i^{\varkappa_i} \tag{1}$$

and

$$\mathtt{E}_i = \hat{e}(\aleph_i, g^{-\varkappa_i})^{\mathfrak{I}} \tag{2}$$

Thereafter, the data $\langle \eth_i, \mathtt{A}_i, \mathtt{E}_i \rangle$ is distributed to individual TU ID_i. According to our design, it is worth noting that the acquired secret information $\eth_i$ for ID_i are considered as the unique partial key that is independently issued by EI, while the remaining partial key value $\varkappa_i$ is preserved during the entire authentication process. Following this way, for $ID_i \in S$, the key set

$$\{(\eth_1, \varkappa_1), (\eth_2, \varkappa_2), \dots, (\eth_t, \varkappa_t)\} \tag{3}$$

with t participating TUs will be one-to-one related to ID_i. That is, each legitimate IoT device maintains the partial key pair for further management. At this point, the offline registration is completed. All the legitimate TUs collect the distinctive partial key $\eth_i$, along with the intermediate value $\langle \mathtt{A}_i, \mathtt{E}_i \rangle$. In this phase, the essential communication rounds between EI and TUs are performed in order to offer mutual verification.

In our design, the proposed group authentication process is assumed to be initialized with one broadcast operation conducted by EI. That is, EI computes $\Lambda = g^{\mathfrak{I}}$ and broadcast $\langle Request, \Lambda \rangle$. In the next, each TU adopts the stored $\langle \eth_i, \mathtt{A}_i, \mathtt{E}_i \rangle$, along with the derived Λ to verify whether the following equation holds:

$$\hat{e}(\mathtt{A}_i, \Lambda)\mathtt{E}_i \overset{?}{=} \hat{e}(\eth_i, \Lambda). \tag{4}$$

If the equation fails, TU stops the procedure and discards the data it has received. Otherwise, TU produces its own partial secret key $\vartheta_i \in \mathbb{Z}_{\mathtt{P}}$ at random and computes $\mathtt{T}_i = \Lambda^{\vartheta_i}$ for the next verification session. In this case, the complete secret key set of TU is presented as $\langle \eth_i, \vartheta_i \rangle$. The previous authentication result is stored as

$$\eta_i = \hat{e}(\mathtt{A}_i, \Lambda)\mathtt{E}_i. \tag{5}$$

Therefore, the identity Tid_i is derived as $Tid_i = \mathtt{A}_i \eth_i{}^{-1} = \zeta_i^{\varkappa_i}$. Meanwhile, the certificate $Auth_i$ can be calculated as $Auth_i = H_2(Tid_i, \mathtt{T}_i, \eta_i)$. In this case, the packet $\langle Tid_i, \mathtt{T}_i, Auth_i \rangle$ is delivered to EI. At this point, EI compares the value Tid_i that was delivered before with its database in order to search for the target TU that matches. It is worth noting that the set $\{\aleph_1^{\varkappa_1}, \dots, \aleph_i^{\varkappa_i}\}$ are previously calculated such that the repetitive operations are prevented. Afterwards, EI is responsible for validating the correctness of the received $Auth_i$, where the value η_i can be calculated according to $\eta_i = \hat{e}(\eth_i, \Lambda)$. If matches, EI computes

$$g^{\vartheta_i} = \mathtt{T}_i g^{-\mathfrak{I}} \tag{6}$$

and uses it in the next group key distribution. The design assigns a widely shared secret key to create a universal group communication channel between EI and all legitimate TUs. Message broadcasting becomes available in this way for practical purposes such as emergency rescue and medical service. Instead of sending the keying message to each device individually, EI sends out a single broadcast to all devices, making key distribution more efficient.

We'll assume that t TUs ($ID_i \in S$) passed the prior EI verification. As a result, the group key should be successfully delivered to all TUs, and outsiders should be unable to deduce the group key via eavesdropping. Accordingly, for $i \in [1,t]$, EI computes

$$\dagger_i = H_3(\hat{e}(g^{\vartheta_i}, \eth_i), \eta_i). \tag{7}$$

Hence $\dagger_i$ is related to certain TU so that EI randomly generates the group key $\zeta \in \mathbb{Z}_{\mathtt{P}}$ and constructs

$$f(x) = (x - \dagger_1) \dots (x - \dagger_t) + \zeta = x^t + \sum_{i=1}^{t-1} d_i x^i + d_0. \tag{8}$$

Notably, for $\forall i \in [1,t]$, $f(x) = \zeta$ holds. Subsequently, EI calculates$\delta = w^{\mathfrak{I}}$ and

$$\wp = H_4(\aleph_i, d_0, \dots, d_{t-1}) \tag{9}$$

and delivers $\langle \delta, \wp, d_0, \dots, d_{t-1} \rangle$. The validation of the following equation:

$$\hat{e}(\delta, g) \overset{?}{=} \hat{e}(w, \Lambda) \tag{10}$$

is conducted in the next. At this point, TU computes

$$\dagger_i = H_3(\hat{e}(g^{\vartheta_i}, \eth_i), \eta_i) \tag{11}$$

and adopts $\dagger_i$ into the calculation as

$$f(\dagger_i) = \zeta, \tag{12}$$

where the distributed group key ζ is derived in TU side. It should be noted that only validated TUs can obtain the right group key ζ using the self-computed $\dagger_i$. The group key is preserved in this way.

5. Security analysis

The proposed authentication design for edge computing environment is evaluated in terms of vital security properties as follows.

5.1. Certificateless authentication

Our technique includes the certificateless authentication feature, which eliminates the requirement for key escrow. For IoT devices, the proposed protocol can allow certificateless authentication. Malicious individuals are unable to expose the TU's private key message. Furthermore, using the collected knowledge, EI is unable to imitate authentic automobiles. According to the previously introduced authentication process, the self-generated random partial key $\vartheta_i \in \mathbb{Z}_{\mathrm{P}}$ from TU side is kept secret to EI all the moment. Moreover, according to DBDH, EI cannot decrypt the correct value of ϑ_i from the received $\mathtt{T}_i = \Lambda^{\vartheta_i}$ as well. In this scenario, impersonation on a certain TU is not achievable.

5.2. Session key construction

To provide data confidentiality and transmission security in an IoT environment, a shared session key must be produced between the EI and all TUs. Our authentication scheme provides the shared session key $\zeta \in \mathbb{Z}_{\mathrm{P}}$ between EI and all the validated TUs. In our design, the final universal key ζ for group communication is managed by EI and then delivered to each valid TU in a secure channel. In this case, the ζ is adopted as the group key between EI and all the legitimate devices that have been verified via mutual authentication. If the existing legitimate IoT evice has not been revoked by EI, the newly distributed session key ζ^{new} can easily be derived by the existing devices with the usage of formula $f(x)$, where

$$f(\dagger_i) = \zeta^{new} \tag{13}$$

holds for all the validated TUs.

5.3. Replay attack resilience

In terms of authentication, the certificate authentication technique is used, with two partial secret keys created by EI and TU respectively: $\langle \eth_i, \vartheta_i \rangle$. As a result, after the successful validation of $Auth_i = H_2(Tid_i, \mathtt{T}_i, \eta_i)$, the used partial secret key $\vartheta_i \in \mathbb{Z}_{\mathrm{P}}$ is chosen at random. In each authenticating session, the partial secret key ϑ_i, as well as the group key $\zeta \in \mathbb{Z}_{\mathrm{P}}$, is considered the randomly generated value. As a result, the previous session's provided $\langle \delta, \wp, d_0, \ldots, d_{t-1} \rangle$ cannot pass the current validation process. In this approach, the replay attack by the malicious entities could be prevented.

5.4. Identity privacy preservation

An adversary (insider/outsider attacker) could conduct illicit tracking towards a specific device in a real-world communication setting, risking the user's privacy. As a result, during the communication process, the true identity of the TU cannot be revealed.

The true identity ID_i of a particular TU i is always hidden in our design. The one-way hashing function H_1 is used in the authentication phase, as demonstrated. The newly constructed temporary identity Tid_i is derived as $Tid_i = \aleph_i^{\varkappa_i}$, which contains the randomly generated parameter $\varkappa_i$. In the EI side, $\varkappa_i$ was previously picked. The sending message $\langle Tid_i, \mathtt{T}_i, Auth_i \rangle$ bears no resemblance to the data exchange that follows. In this method, tracing to a specific device is avoided.

Furthermore, user unlinkability for all participating TUs should be assured, so that the adversary cannot link messages sent by the same TU. The suggested authentication system ensures that TUs are unlinkable and resistant to illicit tracing. That is, the attacker will be unable to track down specific TUs by examining the featured identity in transmitted messages.

5.5. Conditional privacy-preservation

The conditional privacy preservation property is supplied for all legitimate TUs during the whole authenticated key management and data transfer process. If necessary, the central system can reveal the true identify of hostile or compromised entities while maintaining the anonymous identity. In the suggested technique, the anonymous session identities are used in each session, but the confidential original TU identities are kept secret at all times.

Furthermore, as a partial key, the TU chooses a random integer that is only valid and effective for the duration of the current session. On a certain TU, impersonation and forgery will fail the final validation. As a result, the privacy of users is safeguarded. Meanwhile, message retrieval and identity tracking for the selected suspicious TUs can be accomplished, revealing the malicious user behaviors and patterns. Overall, a quite effective authentication and key management system is used to maximize the privacy-preserving property.

As a result, conditional privacy is preserved. To enhance the privacy-preserving property, an effective authentication and key management design, as well as a unique edge communication approach, are implemented. When necessary, the central cloud server may also swiftly divulge each device's true identity. As a result, conditional privacy protection is achieved.

6. Conclusion

In this research, we describe an edge computing-based IoT group association and updating design. The out-of-range IoT devices can be connected to the edge network thanks to the assistance of nearby other devices. The EI side of our architecture's group key updating procedure simply requires modest adjustments, whereas the decryption information of some IoT devices remains constant if the devices have not been revoked. According to the security assessment, the recommended technique can achieve the desired security features.

Declaration of Competing Interest

The authors declare that they have no conflict of interest.

Acknowledgment

The Author would like to thank the editors and reviewers for their dedicated work for this paper.

References

[1] S. Naveen, M.R. Kounte, Key technologies and challenges in iot edge computing, in: 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2019, pp. 61–65, doi:10.1109/I-SMAC47947.2019.9032541.

[2] Z. Zhang, X. Guo, Y. Lin, Trust management method of d2d communication based on RF fingerprint identification, IEEE Access 6 (2018) 66082–66087.

[3] M. Wang, Z. Yan, Privacy-preserving authentication and key agreement protocols for d2d group communications, IEEE Trans. Ind. Inf. 14 (8) (2018) 3637–3647.

[4] P. Mendki, Docker container based analytics at iot edge video analytics usecase, in: 2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU), 2018, pp. 1–4, doi:10.1109/IoT-SIU.2018.8519852.

[5] M. Cao, L. Wang, H. Xu, D. Chen, C. Lou, N. Zhang, Y. Zhu, Z. Qin, Sec-d2d: A secure and lightweight d2d communication system with multiple sensors, IEEE Access 7 (2019) 33759–33770.

[6] M.A. L'opez Peña, I. Muñoz Fernández, Sat-iot: An architectural model for a high-performance fog/edge/cloud iot platform, in: 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), 2019, pp. 633–638, doi:10.1109/WF-IoT.2019.8767282.

[7] D. Kelly, K. Curran, B. Caulfield, Automatic prediction of health status using smartphone-derived behavior profiles, IEEE J. Biomed. Health Inf. 21 (6) (2017) 1750–1760.

[8] M. Alrowaily, Z. Lu, Secure edge computing in iot systems: Review and case studies, in: 2018 IEEE/ACM Symposium on Edge Computing (SEC), 2018, pp. 440–444, doi:10.1109/SEC.2018.00060.

[9] R. Lu, X. Lin, X. Liang, X. Shen, A dynamic privacy-preserving key management scheme for location-based services in VANETs, IEEE Trans. Intell. Transp. Syst. 13 (1) (2012) 127–139.

[10] A. Wasef, X. Shen, EMAP: expedite message authentication protocol for vehicular ad hoc networks, IEEE Trans. Mobile Comput. 12 (1) (2013) 78–89.

[11] H. Aliev, H. Kim, S. Choi, A scalable and secure group key management method for secure v2v communication, Sensors 20 (21) (2020) 6137.

[12] M.N. Aman, U. Javaid, B. Sikdar, A privacy-preserving and scalable authentication protocol for the internet of vehicles, IEEE Internet Things J. 8 (2) (2021) 1123–1139.

[13] Y. Cai, H. Zhang, Y. Fang, A conditional privacy protection scheme based on ring signcryption for vehicular ad hoc networks, IEEE Internet Things J. 8 (1) (2021) 647–656.

[14] T. Miao, J. Shen, C.-F. Lai, S. Ji, H. Wang, Fuzzy-based trustworthiness evaluation scheme for privilege management in vehicular ad hoc networks, IEEE Trans. Fuzzy Syst. 29 (1) (2021) 137–147.

[15] P. Wang, Y. Liu, SEMA: secure and efficient message authentication protocol for vanets, IEEE Syst. J. 15 (1) (2021) 846–855.

[16] L. Wei, J. Cui, Y. Xu, J. Cheng, H. Zhong, Secure and lightweight conditional privacy-preserving authentication for securing traffic emergency messages in VANETs, IEEE Trans. Inf. Forensics Secur. 16 (1) (2021) 1681–1695.

[17] Y. Hao, Y. Cheng, C. Zhou, W. Song, A distributed key management framework with cooperative message authentication in VANETs, IEEE J. Sel. Area. Commun. 29 (3) (2011) 616–629.

[18] L.-Y. Yeh, Y.-C. Chen, J.-L. Huang, ABACS: an attribute-based access control system for emergency services over vehicular ad hoc networks, IEEE J. Sel. Area. Commun. 29 (3) (2011) 630–643.

[19] D. Huang, S. Misra, M. Verma, G. Xue, PACP: an efficient pseudonymous authentication-based conditional privacy protocol for vanets, IEEE Trans. Intell. Transp. Syst. 12 (3) (2011) 736–746.

[20] X. Zhu, S. Jiang, L. Wang, H. Li, Efficient privacy-preserving authentication for vehicular ad hoc networks, IEEE Trans. Veh. Technol. 63 (2) (2014) 907–919.

[21] M. Chuang, J. Lee, TEAM: trust-extended authentication mechanism for vehicular ad hoc networks, IEEE Syst. J. 8 (3) (2014) 749–758.

[22] D. He, S. Zeadally, B. Xu, X. Huang, An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks, IEEE Trans. Inf. Forensics Secur. 10 (12) (2015) 2681–2691.

[23] Q. Feng, D. He, S. Zeadally, K. Liang, BPAS: blockchain-assisted privacy-preserving authentication system for vehicular ad hoc networks, IEEE Trans. Ind. Inf. 16 (6) (2020) 4146–4155.

[24] C. Feng, K. Yu, M. Aloqaily, M. Alazab, Z. Lv, S. Mumtaz, Attribute-based encryption with parallel outsourced decryption for edge intelligent iov, IEEE Trans. Veh. Technol. 69 (11) (2020) 13784–13795.

[25] K. Fan, Q. Pan, K. Zhang, Y. Bai, S. Sun, H. Li, Y. Yang, A secure and verifiable data sharing scheme based on blockchain in vehicular social networks, IEEE Trans. Veh. Technol. 69 (6) (2020) 5826–5835.

[26] M.O. Ozcan, F. Odaci, I. Ari, Remote debugging for containerized applications in edge computing environments, in: 2019 IEEE International Conference on Edge Computing (EDGE), 2019, pp. 30–32, doi:10.1109/EDGE.2019.00021.

[27] S.K. Datta, C. Bonnet, An edge computing architecture integrating virtual iot devices, in: 2017 IEEE 6th Global Conference on Consumer Electronics (GCCE), 2017, pp. 1–3, doi:10.1109/GCCE.2017.8229253.

[28] J. Xu, S. Wang, A. Zhou, F. Yang, Edgence: A blockchain-enabled edge-computing platform for intelligent iot-based dapps, China Commun. 17 (4) (2020) 78–87, doi:10.23919/JCC.2020.04.008.

[29] D. Loghin, L. Ramapantulu, Y.M. Teo, On understanding time, energy and cost performance of wimpy heterogeneous systems for edge computing, in: 2017 IEEE International Conference on Edge Computing (EDGE), 2017, pp. 1–8, doi:10.1109/IEEE.EDGE.2017.10.

[30] J. Xu, B. Palanisamy, H. Ludwig, Q. Wang, Zenith: Utility-aware resource allocation for edge computing, in: 2017 IEEE International Conference on Edge Computing (EDGE), 2017, pp. 47–54, doi:10.1109/IEEE.EDGE.2017.15.

[31] M. Goudarzi, H. Wu, M. Palaniswami, R. Buyya, An application placement technique for concurrent iot applications in edge and fog computing environments, IEEE Trans. Mobile Comput. 20 (4) (2021) 1298–1311, doi:10.1109/TMC.2020.2967041.

[32] Q. Liu, L. Cheng, T. Ozcelebi, J. Murphy, J. Lukkien, Deep reinforcement learning for iot network dynamic clustering in edge computing, in: 2019 19th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID), 2019, pp. 600–603, doi:10.1109/CCGRID.2019.00077.

[33] X. Liu, J. Yu, Z. Feng, Y. Gao, Multi-agent reinforcement learning for resource allocation in iot networks with edge computing, China Commun. 17 (9) (2020) 220–236, doi:10.23919/JCC.2020.09.017.