Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 9921036, 14 pages
https://doi.org/10.1155/2021/9921036

Research Article

Efficient Authentication for Internet of Things Devices in Information Management Systems

Xiaofeng Wu,[1] **Fangyuan Ren**,[2,3] **Yiming Li**,[2] **Zhenwei Chen**,[2] **and Xiaoling Tao**[4]

[1]*School of Management, Xi'an Jiaotong University, Xi'an 710049, China*
[2]*School of Cyberspace Security, Xi'an University of Posts and Telecommunications, Xi'an 710121, China*
[3]*Du Xiaoman Financial, Beijing 100089, China*
[4]*Guangxi Cooperative Innovation Center of Cloud Computing and Big Data, Guilin University of Electronic Technology, Guilin 541004, China*

Correspondence should be addressed to Fangyuan Ren; rfyren@163.com

Received 22 March 2021; Accepted 7 July 2021; Published 19 July 2021

Academic Editor: Ximeng Liu

Copyright © 2021 Xiaofeng Wu et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

With the rapid development of the Internet of Things (IoT) technology, it has been widely used in various fields. IoT device as an information collection unit can be built into an information management system with an information processing and storage unit composed of multiple servers. However, a large amount of sensitive data contained in IoT devices is transmitted in the system under the actual wireless network environment will cause a series of security issues and will become inefficient in the scenario where a large number of devices are concurrently accessed. If each device is individually authenticated, the authentication overhead is huge, and the network burden is excessive. Aiming at these problems, we propose a protocol that is efficient authentication for Internet of Things devices in information management systems. In the proposed scheme, aggregated certificateless signcryption is used to complete mutual authentication and encrypted transmission of data, and a cloud server is introduced to ensure service continuity and stability. This scheme is suitable for scenarios where large-scale IoT terminal devices are simultaneously connected to the information management system. It not only reduces the authentication overhead but also ensures the user privacy and data integrity. Through the experimental results and security analysis, it is indicated that the proposed scheme is suitable for information management systems.

1. Introduction

With the advancement of various wireless mobile network technologies, the field of Internet of Things (IoT) has developed rapidly. IoT is connected by multiple smart physical devices through the Internet. The IoT is used in many different fields, such as smart homes, smart cities, smart health, Internet of Vehicles, and information management systems (IMS). In IMS, IoT devices serve as an information collection and exchange unit. The IoT device plays an important role in connecting users and systems so that they can interact. Furthermore, the IMS requires a large amount of information transmission and management. However, these IoT devices send and receive highly sensitive data regarding the privacy of users or other information regarding the movement of users from one location to another location [1]. Therefore, the primary problem is to solve the efficiency and security of identity authentication in the system. In the field of information and communication technology, the IMS needs a systematic model that contains multiple information processing units to realize. The current development of Internet and wireless network technology has brought us various convenient network services, but at the same time, it has also brought many new security threats. For example, the intrusion of the Internet system leads to information security leakages and other related incidents, which have caused various enterprises in different fields to attach great importance to the security of IMS. In an IMS, users, IoT devices, computers, and servers make up the various parts of the system. These components are used to complete information processing operations such as access, collection, storage, and transmission of information. The use of IMS

enables information to be systematically carried out in batches and secure operations, thereby improving work efficiency. Since the information is transmitted in the wireless network environment, the user's identity information and the content of the message will be exposed on the network. Therefore, the system also has some security problems. Attackers can use the loopholes in the IMS to illegally invade the system, steal, tamper with, and destroy confidential information. For example, an attack on an enterprise's IMS will cause unpredictable losses to the enterprise. Hence, privacy protection is particularly important. The security requirements of the IMS are listed below.

(1) Confidentiality: to protect information from eavesdropping by illegal users to prevent passive attacks

(2) Completeness: to protect information content from being illegally tampered with and ensure that the system is not subject to malicious tampering, sabotage, and other active attacks

(3) Nonrepudiation: the sender and receiver of the information cannot deny the fact that they have sent or received the information

(4) Reliability: ensure that the system or server will not be illegally interfered, faked, and affected by other deceptive behaviors for the normal operation of the system

(5) Availability: ensure that all authorized users can access the information management system normally without denial of service attacks

Therefore, given the information security of the IMS, the mutual authentication between the user and the server must be performed first before the user accesses the system. After both parties have passed the authentication, the access and transmission of information in the system can continue to be allowed. Some elliptic curve cryptography- (ECC-) based certification schemes have been used in the IMS of an enterprise. For example, an authentication protocol based on the elliptic curve discrete logarithm problem (ECDLP) [2] was proposed. However, this scheme has the defect that cannot resist tracking attacks and forgery attacks. Then, Islam et al. [3] proposed an advanced scheme based on ECDLP, which has made improvements to the previous problems, and it can effectively resist tracking attacks. However, this scheme needs to update the database during the identity authentication phase, which increases the cost of the back-end server and does not have the feature of mutual authentication. Therefore, there is an urgent need for a secure data transmission and authentication scheme that can guarantee user privacy in IMS. Users' operations such as accessing data information in the IMS are usually performed by connecting smart terminal devices to the network, such as mobile phones, computers, and other IoT devices. Hou et al. [4] proposed a novel blockchain-based architecture for IoT data sharing systems. For the IoT, user access control becomes crucial because of the characteristics of the IoT. To address this issue, Shobhan et al. [5] proposed a new three-factor certificateless-signcryption-based user access control for the IoT environment. For different wireless network technologies and application scenarios, the security issues faced are different. In terms of 5G security research, the Third Generation Partnership Project (3GPP), the 5G Infrastructure Public Private Partnership (5G PPP), the Next Generation Mobile Networks (NGMN), the International Telecommunication Union (ITU-2020) promotion group, Ericsson, Nokia, and Huawei also released their own 5G security requirements white papers [6–10]. Today, with the gradual development and popularization of 5G network technology, IMS can also run on 5G networks. In the 5G environment, problems such as the disclosure of user identity information and the exposure of data to relatively open channels due to big data. Thus, secure data transmission under the 5G network has become one of the research hotspots since the development of the fifth-generation communication technology.

With the promotion and commercial application of 5G communication technology by the three major telecommunication operators, people's demand for mobile intelligent devices increases. The computing power and storage capacity of smart mobile devices are limited. When the cost of authentication process is large, they are often unable to calculate the complex authentication process. In the process of authentication, some data such as location data needs stronger protection. Once these data are leaked, it may cause great loss [11]. In some application scenarios, fine-grained access control and the identity-based encryption are urgently needed [12]. In another application scenarios, intelligent mobile devices need to switch authentication frequently. Therefore, a more rapid and secure authentication process is urgently needed. With the development of cloud computing and cloud storage technology, the authentication process of intelligent mobile devices can also be completed by relying on cloud computing technology to improve the authentication efficiency [13]. In addition, the traditional authentication mode is not suitable for equipment to equipment authentication, which can achieve the security of end-to-end authentication and reduce the need of computing cost ripple [14]. In the application scenario of unstable network or no network, offline authentication can improve the reliability of device authentication.

Due to the 3GPP 5G network has the characteristics of high capacity and low transmission delay, it has the advantages of high energy saving level, high efficiency, and relatively low expense. Access to the 5G network environment brings convenient network services, but it also creates more security challenges. These can just meet the user's requirements for transmission message delay and service quality in IMS. Now, 5G has become the focus of more and more researchers [15, 16]. By introducing RUSH, Zhang et al. [17] proposed a robust and universal seamless handover authentication scheme for 5G heterogeneous networks. In RUSH, it introduces the blockchain technology [18] and chameleon hash function to realize an anonymous authentication key protocol for handover in various scenarios.

With the advent of the era of intelligent information society, users' demands are also changing constantly. In order to meet various demands, the IoT technology has been

constantly developed and has become more closely connected with people's life. When each user accesses information in an IMS, one or more IoT devices are usually connected to the network to send or receive messages. It has become a trend that more intelligent terminal devices are designed to provide a range of services that need to be achieved by connecting to the network. The IMS under the 5G network will support simultaneous access by a large number of users and devices without causing the current system crash when multiple users access at the same time. IMS access to 5G will not only greatly increase users' access efficiency but also provide security to protect the user's identity information from being leaked. At the same time, it also prevent illegal attacks during the transmission of massive information. The 5G security mechanism should not only ensure the security of massive access devices but also ensure that the information of users will not be leaked when they interact with the network in the scenario of IoT device access. The function of these IoT terminals is generally to collect sensitive data and usually to transmit it. When users need to access an IMS, these IoT devices serve as a medium for transmitting requests and receiving information. Once the data is leaked, it will not only bring huge losses to users but also seriously affects the 5G network. In addition, if large-scale terminals access the network at the same time and the network authenticates each terminal one by one. It will make the authentication cost too high, the network is difficult to bear, and its authentication efficiency will also be unsatisfactory. The actual identity of the user needs to meet certain anonymity under specific scenario requirements. Hence, data privacy and security are particularly important during access authentication and data transmission. Therefore, in most of the technology research especially those related to 5G security access authentication technology, both communication and security requirements should be considered. On the premise of ensuring communication performance, considering the massive access terminals of 5G network and the diversification of security threats, different security access authentication schemes should be adopted.

2. Related Work

In the Long-Term Evolution-Advanced (LTE-A) networks, many protocols are formulated for access security issues [19–27]. In addition, many researchers are paying attention to security of IoT deployment under the 5G network or some other advanced architecture [28–31]. According to the research findings, the current research on a large number of equipment access authentication process in the network, and these schemes are mainly categorized into the following two types.

(i) Group-based security context transformation

Through this type of scheme, many researchers have proposed some group-based access authentication schemes [19–23]. Based on the problem of a large number of users roaming to the same service network when receiving services, Chen et al. first proposed such a group access authentication and key agreement scheme [19]. In the IoT scenario, in order to ensure that information is not leaked and safe, authentication is required. In practice, however, we usually need to process information from multiple IoT devices at the same time. Obviously, one-to-one certification has great limitations in terms of timeliness and complexity. Therefore, we need to perform group authentication [20, 21]. The access authentication process of SE-AKA Scheme [22] and EG-AKA Scheme [23] is similar to Lai's scheme, and temporary group key is used to realize local identity authentication. These schemes can reduce the cost of high communication costs between home network and service networks by simplifying the process when dealing with the authentication of other group members. However, they are still unable to avoid signaling congestion since they still need to send multiple access request messages to connect to the network.

(ii) Group-based aggregation authentication

In group-based aggregation authentication scheme, a large number of devices are first combined to create a group, and a group leader is selected at the same time. When multiple members from an IoT group need to access the network at the same time, they all issue an access request message. The group leader then gathers the messages of these group members into an access request message and sends them to the network. The verifier in the network then validates the aggregated signature message, thus validating the entire group of devices or aggregate message authentication code generated by the group leader. In Cao's scheme, a group-based aggregate signature authentication scheme is proposed for the first time [24]. Whereafter, a lightweight packet protection protocol based on aggregated message authentication codes is proposed by Lai et al. [25]. Based on secret sharing technology, Li et al. proposed a new group-based protocol with dynamic policy update [26]. Through aggregation technology, Cao's scheme [24] and Li's scheme [26] made great optimizations in terms of communication and signaling overhead. However, both of these schemes may generate a lot of computational overhead. Basudan et al. proposed a protocol [27]. This protocol is a data security transfer protocol based on fog computing and also has the attribute of privacy protection. This scheme can not only make the signaling cost low but also ensure the authenticity and confidentiality of the design. However, derived from the protocol by introducing bilinear pairing operations, a large amount of computing cost is caused. In the case of limited equipment power, they are not suitable. Lightweight authentication in Lai's scheme can be achieved by using symmetric cryptography. However, due to the existence of internal forgery attack, there are still many security vulnerabilities such as DoS attack and lack of identity privacy protection security issues in LGTH scheme. Aiming at these problems, Zhang et al. proposed a multiparty authentication scheme [28]. This scheme adopts certificateless signcryption authentication technology to solve the problems in the multidevice access scenario. It not only realizes the access authentication of multiple devices but also achieves the characteristics of protecting user

identity privacy and nonrepudiation. But this scheme cannot realize mutual authentication between the user and the server. Moreover, there is the problem of a huge number of messages in the network, which easily causes network congestion. Therefore, the authentication overhead and signaling overhead are relatively large.

These two approaches mentioned above still have some issues with both performance and security issues, although they can reduce signaling overhead to some extent. In addition, these schemes do not address the process of secure data transfer, but simplify the process of access authentication.

2.1. Our Contributions. An efficient and secure authentication protocol for IoT devices in IMS is proposed in this paper in which a CS is introduced for file management. Our main contributions are summarized as follows:

(i) Considering the current development status of wireless communication technology and the mobility and efficiency of most IoT devices, we decided to connect IMS to the 5G network. We will perform our protocol between IoT devices and AMF to achieve mutual authentication. After the mutual authentication process, data can be transmitted in a secure manner under 5G-based IMS

(ii) Our scheme is to build an IoT group. The leader of the group will aggregate the messages of the legitimate group members and send them to the network, which greatly reduces the number of messages sent to the network and effectively avoids network congestion in IMS. All IoT devices need to be registered on the network before the device is connected to the system. In this stage, the proposed scheme introduces a group leader. It can also realize that AMF communicates to each IoT member device in the group through the group leader device (GLD)

(iii) Data transmission and authentication are carried out under the premise of ensuring the security and integrity of data. In our scheme, the method of certificateless aggregation and signcryption is adopted. And the group session key (GSK) is used to encrypt messages between the network and the IoT group

(iv) Mutual authentication between terminal and network will be implemented in our scheme. It can ensure not only the legality of the terminal accessing the network but also the authentication of the network, and the server is realized

(v) The network inspects the legitimacy of the entire IoT group and the integrity of the transmitted data through aggregate signcryption, which significantly improves the authentication efficiency. The security analysis shows that the scheme can resist security threats such as replay attack and forgery attack. The performance analysis indicates that the scheme is better than the existing schemes in signaling cost, computing cost, and communication cost when facing the massive IoT devices and can take into account the security and efficiency

2.2. Organization. The following arrangement of the paper is shown below. In Section 3, we elaborated an overview of the system model and relevant requirements. In Section 4, we give a comprehensive overview of the scheme proposed in this paper. The security analysis part and the performance evaluation part are, respectively, described in detail in Section 5 and Section 6. Finally, the conclusion and future work are given in Section 7.

3. Model and Security Requirements

3.1. System Model. When designing the system model, it is necessary to consider the actual needs of communication, user terminal, and network communication. In addition, timeliness is also critical for communication. An IMS usually consists of an authentication server, a confidential server, a file server, and a client. When a user logs in and accesses the file system through a client running on a personal computer, it must first pass the authentication of the authentication server. In a system with high confidentiality, file information also needs to be encrypted by a confidential system. The most important thing in the process of the system running in the 5G environment is security and efficient mutual authentication and data transmission.

Generally, a large enterprise or organization needs to handle a huge amount of data and the number of users for information management. Therefore, a management entity with a large storage capacity is required, and the server must not be interrupted. Then, a management entity that can operate continuously is required. The important issue that the information management department must face is to ensure the data security and stable operation of the information management system. In our scheme, we overcome the problem of large storage and computing overhead by introducing cloud servers and the service interruption will not occur. In addition, the introduction of cloud servers can also avoid data loss or system crashes caused by hardware damage. There are four types of entities in an IMS system model: the Key Generation Center (KGC), the Access and Mobility Management (AMF), the Cloud Sever (CS), and IoT groups as shown in Figure 1. In this system, AMF is used as the authentication server, the security server is assumed by KGC, a CS is introduced to complete the work related to the file server, and there are multiple groups (i.e.group_i, $i = 1, 2, 3, \cdots, n$) of IoT devices that make up the IMS client. These entities can be roughly divided into three parts: information access unit, information transmission unit, and information processing unit.

(1) The information access unit is composed of multiple IoT devices of the user, these IoT devices are divided into multiple IoT groups according to specific attributes. And this unit mainly forms human-computer interaction with the user, allowing the user to access the IMS through the IoT device and perform related operations on the information stored in the IMS

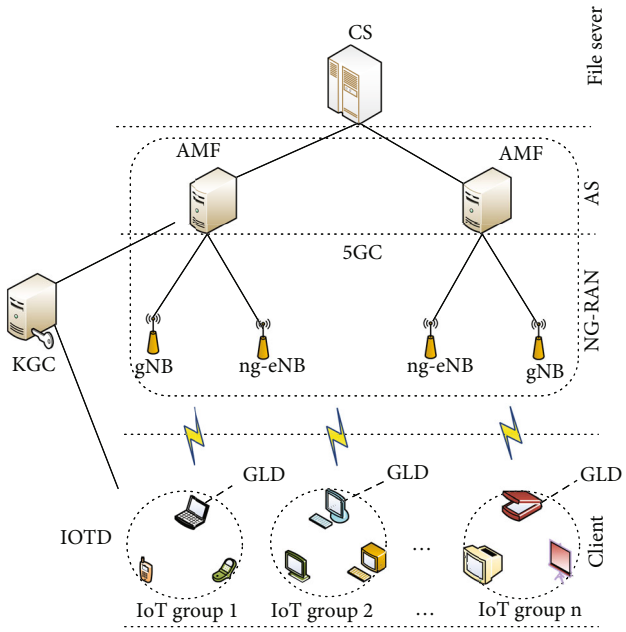

Figure 1: The system model of 5G-enabled information management system.

(2) The information transmission unit is composed of two types of access points in NG-RAN, namely, gNB and ng-eNB. This part, like the base station, is mainly responsible for user access to the network. It is also a medium for sending and receiving information and communicating

(3) The information processing unit is composed of three types of servers, KGC, AMF, and CS. This part mainly completes the authentication of user identity information, the encryption of data messages, and the function of processing the information stored in the server

The communication of the whole system includes communication between IoT device (IOTD) and KGC, AMF and KGC, IOTD and group leader of its IoT group, each IoT group and AMF, and AMF and CS. In our scheme, KGC is an incomplete trusted entity. It generates partial key during the interaction with IOTD and verifies whether the registered IOTD is legitimate and whether it is a corresponding group member. IOTD encrypts the communication data and sends it to the GLD of the IoT group for verification and aggregation. After that, the GLD sends the aggregate data of the whole group to the network through ng-ran, and AMF verifies the legitimacy of the entire IoT group. Various information of IMS is stored in CS, and users access data information in CS indirectly through AMF, because the communication between the AMF and the CS can be regarded as a completely trusted transmission, and mutual authentication can be performed between the AMF and the IOTD. The specific process is as described later. First, AMF selects a third-party cloud service operator to register and configure the cloud server and then establish the session key after passing the mutual authentication between IOTD and AMF. Finally, AMF accesses the information in CS and sends it to each IOTD.

3.2. Security and Privacy Requirements. In IMS, users access the data in the file server through the IOTD accessing the system network. In this scheme, IMS is based on the 5G wireless network, so IoT devices access the system network through the nodes gNB and ng-eNB of the 5G access network. Since this process is carried out in a wireless network environment, there are some insecure elements of the connected node between IoT devices and networks can be derived from the system model presented above. And the external adversaries want to interfere with wireless transmission via control and disrupt the medium between IoT devices and networks. On the one hand, attackers can attack in a range of insecure means including replay attacks, man-in-the-middle attacks, and simulation attacks to simulate IoT devices or networks to launch various protocol attacks. On the other hand, privacy protection is indispensable for the sender. Therefore, the identity of the IOTD and the IoT group must have good concealment during the access of authentication. Even if the attacker is threatened, the real identity of the IOTD cannot be obtained.

Specifically, the following safety requirements should be met in the design proposal.

(1) Mutual authentication: when the network is sent an access request by a group of IoT devices and needs to be accessed, AMF also authenticates the group of devices. In addition, each IOTD needs to confirm the legitimacy of AMF

(2) Identity privacy protection: in the process of data transmission of IoT group, mutual authentication of network is usually accompanied. In order to ensure that the attacker will not steal the identity information and group identity information of the IOTD, the actual identity and group identity information of each IOTD need to be hidden in the message

(3) Resistance to protocol attacks: typically, the scheme needs to resist various existing protocol attacks, such as replay, eavesdropping, and man-in-the-middle attacks

(4) Data confidentiality and integrity: in general, the confidentiality and integrity of data transmission between the IoT group and the AMF should be guaranteed. Based on this, scheme can be designed

(5) Efficient and feasible: the proposed scheme needs to reduce all kinds of costs in the process of authentication, including calculation cost, signaling cost, and communication cost

4. The Proposed Authentication Scheme

The efficient authentication for Internet of Things devices in information management systems consists of seven

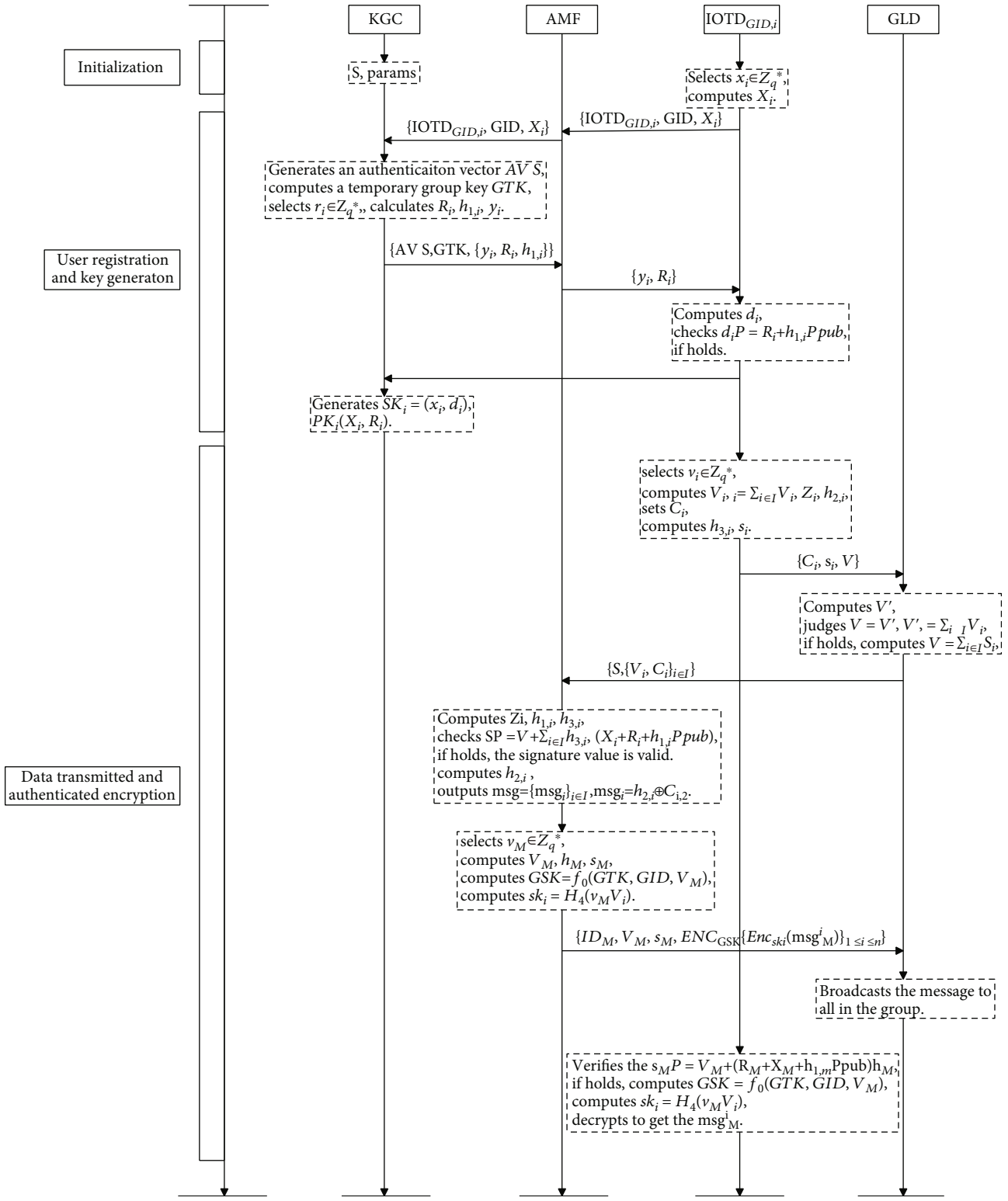

Figure 2: The procedures of the proposed scheme.

algorithms: system initialization, client key extraction, private key extraction, signcryption, aggregate signcryption, authentication, and aggregate authentication. The detailed process is shown in Figure 2.

(1) System Initialization: input security parameters λ, the algorithm can return a series of system public parameters, and the master private key from the input value

(2) Client Key Extraction: the user ID_i first chooses a random number x_i and then computes the common parameters X_i

(3) Private Key Extraction: after KGC receives (ID_i, X_i), it randomly selects r_i and calculates R_i, Y_i, y_i and set the private key (x_i, y_i) and public key (X_i, Y_i)

(4) Signcryption: ID_i signcrypts the message m_i and send the signcryption to the receiver B as the identity ID_B

(5) Aggregate Signcryption: after receiving signcrypts, B aggregates signcrypts and generates aggregate signcryption and sends them to verifier A

(6) Authentication: B authenticates the signcryption after receiving the signcryption of the message m_i

(7) Aggregate authentication: verifier A authenticates the aggregate signcryption after receiving the aggregate signcryption sent by B

The process of this scheme can be divided into the following three stages: initialization phase, user registration and key generation phase, and data transmitted and authenticated encryption phase.

4.1. Initialization Phase. During the system initialization phase, KGC executes the system initialization algorithm to generate the system common parameters params and master key. The detailed process is as follows:

(1) KGC selects a cyclic additive group G of prime order q when it receives a security parameter λ. Suppose P is the generator of G

(2) Then, KGC chooses four hash functions $H_0 = \{0,1\}^{\ell_1} \longrightarrow Z_q^*$, $H_1 = \{0,1\}^{\ell_2} \longrightarrow Z_q^*$, $H_2 = \{0,1\}^* \times G$, and $H_3 = G \longrightarrow Z_q^*$, where ℓ_1 is the bit length of the user and ℓ_2 is the bit length of the plain text message

(3) KGC chooses $s \in_R Z_q^*$ as the master key and computes $P_{\text{pub}} = sP$

(4) Finally, the $\{G, P, q, P_{\text{pub}}, H_{i\{0\le i\le 3\}}\}$ is used as the public parameter, and for KGC, the master key remains his private secret

4.2. User Registration and Key Generation Phase. In this stage, each IOTD and AMF start to register and provide some of the private keys to obtain another part of the private key generated by KGC. Then, KGC sends a message to the IOTD and AMF, respectively; the content is their corresponding private key. Each user legally has a distinctive *ID*, and each user has one or more terminal devices. Thus, multiple different devices constructed into an Internet of Things group should have common attributes. These common attributes are user attribution consistency, location consistency, functional similarity, or other similar characteristics. A GLD can be selected, which is based on the corresponding capabilities (such as the communication capabilities of each device, storage status, and battery status). In the 5G network, GLD will be activated at the same time when data is sent and received between the network and the user equipment. There is a dedicated group identity (GID) and a group key (GK) between each device and KGC that is prestored in the IoT group. And there are many IoT groups, one of these groups is denoted as $\text{group}_i (i = 1, 2, 3 \cdots n)$. Each IOTD has an identity IOT $\text{D}_{\text{GID},i}$, let $\text{IOTD}_{\text{GID},1}$, $\text{IOTD}_{\text{GID},2}$,...,$\text{IOTD}_{\text{GID},n}$ be a member of the group_i. This stage is illustrated as follows.

(1) $\text{IOTD}_{\text{GID},i}$ randomly selects $x_i \in_R Z_q^*$ and computes $X_i = x_i P$. Then, a message containing the terminal identification $\text{IOTD}_{\text{GID},i}$, the group identity GID, and X_i is sent to AMF

(2) Upon receiving the message, AMF transmits the identity verification request message to KGC, which contains the terminal identification $\text{IOTD}_{\text{GID},i}$, the group identity GID, and X_i

(3) When a message is received from the sender, KGC begins to validate the received terminal identification $\text{IOTD}_{\text{GID},i}$ and GID validate the terminal $\text{IOTD}_{\text{GID},i}$ as a member and also validate whether it is a member of group. Then, the KGC generates an authentication vector AVS and defines the $\text{GTK} = f_0(\text{GK}, \text{GID})$ as a temporary group key. Then, select a secure hash function f_0 safely, which is confidential between the IoT group, AMF, and KGC. Almost simultaneously, the KGC randomly selects $r_i \in_R Z_q^*$ and calculates $R_i = r_i P$, $h_{1,i} = H_1(\text{IOTD}_{\text{GID},i} \| X_i \| R_i \| \text{GID})$ and $y_i = r_i + sh_{1,i} + H_0(sX_i)$. Finally, the KGC embeds AVS, GTK, and $(y_i, R_i, h_{1,i})$ in the authentication response message sent to AMF

(4) When the AMF receives the response message, (y_i, R_i) will be sent to $\text{IOTD}_{\text{GID},i}$

(5) When a message is received from the AMF, IOT $\text{D}_{\text{GID},i}$ computes $d_i = y_i - H_0(x_i P_{\text{pub}})$ and checks the equation $d_i P = R_i + h_{1,i} P_{\text{pub}}$. If the equation hold, the KGC generates the complete key $SK_i = (x_i, d_i)$, $PK_i = (X_i, R_i)$.

The following details show that AMF generates key pairs in a similar way to the $\text{IOTD}_{\text{GID},i}$.

(1) Assume that the ID_M as an identity of the AMF, it selects a random number $x_M \in_R Z_q^*$ and calculates

$X_M = x_M P$. After the above calculation is completed, the request message is sent to KGC. The message includes its identity ID_M and X_M

(2) After receiving the message. The KGC validates the ID_M by validating the messages it receives that contain ID_M and X_M. Then, the KGC generates an authentication vector AVS_M. At the same time, the KGC randomly selects $r_M \in_R Z_q^*$ and computes $R_M = r_M P$, $h_{1,M} = H_1(sn_M \| X_M \| R_M)$ and $y_M = r_M + sh_{1,M} + H_0(sX_M)$. Finally, the KGC embeds AVS_M and $(y_M, R_M, h_{1,M})$ in the authentication response message sent to AMF

(3) When AMF receives a message from the KGC, it computes $d_M = y_M - H_0(x_M P_{\text{pub}})$ and checks the equation $d_M P = R_M + h_{1,M} P_{\text{pub}}$. If the equation hold, KGC generates the complete key $SK_M = (x_M, d_M)$, $PK_M = (X_M, R_M)$.

4.3. Data Transmitted and Authenticated Encryption Phase. In this part, the IoT groups and the AMF perform data encryption and transmission operations while encrypting and transmitting data. And the CS we introduced is through a third-party cloud-computing technology operator such as Amazon, Alibaba Cloud, and Google. Then, each IoT group and AMF can perform mutual authentication. When the IOTD is connected to the network, GLD will aggregate the encrypted data and verification information of each member in the group. And the GLD of each group generates an aggregate signcryption. Then, AMF will send aggregated information and other public parameters by GLD. Based on the aggregated signcryption information, AMF can verify IoT members in each group. A key will be established between each terminal device and the AMF to ensure the security of the data. When the IoT group and the AMF interact, and the group session key GSK will be obtained. Subsequently, AMF uses its private key to generate a signature and send the encrypted data. After the authentication is passed, the user can access the data in the CS. The process is described in detail as follows; we assume that the following steps are executed in a certain group (i.e.group_i). And other groups are similar.

(1) In a $\text{group}_i (i = 1, 2, 3 \cdots n)$, each $\text{IOTD}_{\text{GID},i}$ will select an element $v_i \in_R Z_q^*$. Then, five steps will be performed in proper order

(a) Computes $V_i = v_i P$ and sends it to other $n-1$ group members

(b) Computes $V = \sum_{i \in I} V_i$, $Z_i = v_i(R_M + h_{1,M} P_{\text{pub}})$, $h_{2,i} = H_2(ID_M \| V_i \| V \| v_i X_M)$

(c) Sets $C_i = C_{i,1} \| C_{i,2} = \text{IOTD}_{\text{GID},i} \| \text{GID} \| (h_{2,i} \oplus \text{msg}_i)$

(d) Computes $h_{3,i} = H_3(V_i \| C_i \| X_i \| R_i \| Z_i)$

(e) Computes $s_i = v_i + (d_i + x_i) \cdot h_{3,i}$

(2) $\text{IOTD}_{\text{GID},i}$ sends the above ciphertext C_i, the signcryption s_i, and V embedded access request message to GLD in the group_i

(3) After receiving messages from other group members in group_i, the GLD judges whether V and V' are equal, where $V' = \sum_{i \in I} V_i$ and if $V = V'$, computes $S = \sum_{i \in I} s_i$, and sends the aggregated message $\{S, \{V_i, C_i\}_{i \in I}\}$ to AMF

(4) The GLD of each group sends an aggregate message to the AMF. And then for the group_i, AMF begins to execute the following six steps. Similarly, it performs the same operation for each IoT group

(a) Computes $Z_i = d_M V_i$

(b) Sets $h_{1,i} = H_1(\text{IOTD}_{\text{GID},i} \| X_i \| R_i \| \text{GID})$.

(c) Sets $h_{3,i} = H_3(V_i \| C_i \| X_i \| R_i \| Z_i)$.

(d) Then, AMF can check whether the formula $SP = V + \sum_{i \in I} h_{3,i}(X_i + R_i + h_{1,i} P_{\text{pub}})$ is equal. The detailed calculation process is as follows

$$\begin{aligned} SP &= \Sigma_{i \in I}(v_i + (d_i + x_i) \cdot h_{3,i}) P \\ &= \Sigma_{i \in I}\left(v_i + \left(y_i - H_0\left(x_i P_{\text{pub}}\right)\right) + x_i \cdot h_{3,i}\right) P \\ &= \Sigma_{i \in I}(v_i + (r_i + s \cdot h_{1,i} + x_i) \cdot h_{3,i}) P \\ &= \Sigma_{i \in I} V_i + \left(R_i + P_{\text{pub}} \cdot h_{1,i} + X_i\right) \cdot h_{3,i} \\ &= V + \Sigma_{i \in I}\left(X_i + R_i + P_{\text{pub}} \cdot h_{1,i}\right) \cdot h_{3,i}. \end{aligned} \tag{1}$$

We say that the signature value is valid if the equation holds. The AMF can ensure that the received ciphertext C_i is not only valid but also belongs to a legal $\text{IOTD}_{\text{GID},i}$ in the group_i.

(e) Computes $h_{2,i} = H_2(ID_M \| V_i \| V \| x_M V_i)$

(f) AMF produces an output $\text{msg} = \{\text{msg}_i\}_{i \in I}$, where $\text{msg}_i = h_{2,i} \oplus C_{i,2}$

(5) If the data in the CS needs to be sent to an IOTD, it needs to be sent through AMF. AMF reads the data directly from the preregistered and configured CS and then sends the read data to IOTD_(GID, i) in the group_i. After that, AMF performs the following steps

(a) Selects an element $v_M \in_R Z_q^*$, then three values will be calculated, and they are $V_M = v_M P$, $h_M = H_2(ID_M \| V_M \| GID)$, $s_M = v_M + (d_M + x_M) \cdot h_M$

(b) Computes $\text{GSK} = f_0(\text{GTK}, \text{GID}, V_M)$ as the session key with GLD to encrypt the message msg_M

(c) Computes $sk_i = H_4(v_M \cdot V_i)$ as the session key with $\text{IOTD}_{\text{GID},i}$ to encrypt msg_M^i

Table 1: The symbol of notation.

Symbol	Definition
N_g	A quantity of groups
N_t	A quantity of terminals

Table 2: The signaling overhead.

Protocol	The number of signaling
Cao's scheme	$7N_t + 3N_g$
Sultan's scheme	$N_t + N_g$
Our scheme	$N_t + 3N_g$

(d) Generates an aggregate message $(ID_M, V_M, s_M, \mathrm{ENC}_{\mathrm{GSK}}\{\{\mathrm{ENC}_{\mathrm{sk}_i}(\mathrm{msg}_M^i)\}\}_{1\le i\le n})$ and send the aggregate message to GLD

(e) After receiving the message, GLD broadcasts the message to all in the group

(f) $\mathrm{IOTD}_{\mathrm{GID},i}$ verifies that the following equation is true: $s_M P = V_M + (R_M + X_M + h_{1,M} \cdot P_{\mathrm{pub}}) \cdot h_M$. The detailed process is as follows

$$\begin{aligned} s_M P &= (v_M + (d_M + x_M) \cdot h_M) P \\ &= v_M P + (d_M P + x_M P) \cdot h_M \\ &= V_m + ((r_M + s \cdot h_{1,M}) P + x_M P) \\ &= V_M + \left(R_M + X_M + h_{1,M} \cdot P_{\mathrm{pub}}\right) \cdot h_M. \end{aligned} \tag{2}$$

If the equation holds, computes $\mathrm{GSK} = f_0(\mathrm{GTK}, \mathrm{GID}, V_M)$, $sk_i = H_4(v_M \cdot V_i)$, and decrypts to get the message ms g_M^i.

5. Security Analysis

In this part, the security of the protocol has been analyzed. And we have defined six security goals.

(1) Mutual authentication: in the IoT group and AMF, mutual authentication can be implemented in our scheme. In the process of AMF's identity authentication for each $\mathrm{IOTD}_{\mathrm{GID},i}$, the legal signcryption s_i is generated only by the convincing IOTD, and GLD calculates the valid aggregate signature. If the adversary does not have a correct private key, it is impossible to obtain a valid aggregate value. In addition, a private key can be used to generate a signcryption to authenticate the AMF

(2) Data privacy and integrity: in order to strengthen data security, our scheme uses certificateless aggregation and signcryption technology. When data is transferred from $\mathrm{IOTD}_{\mathrm{GID},i}$ to AMF, only legitimate users have a valid private key. And the legal public key of AMF is jointly used to signcrypt the data. This operation is run by GLD. And only legal AMF can verify the aggregate signcryption and decrypt it. In addition, when the data is transmitted from AMF to $\mathrm{IOTD}_{\mathrm{GID},i}$, use the session key of each $\mathrm{IOTD}_{\mathrm{GID},i}$ and AMF (IoT group and AMF) to ensure the privacy and integrity of the data

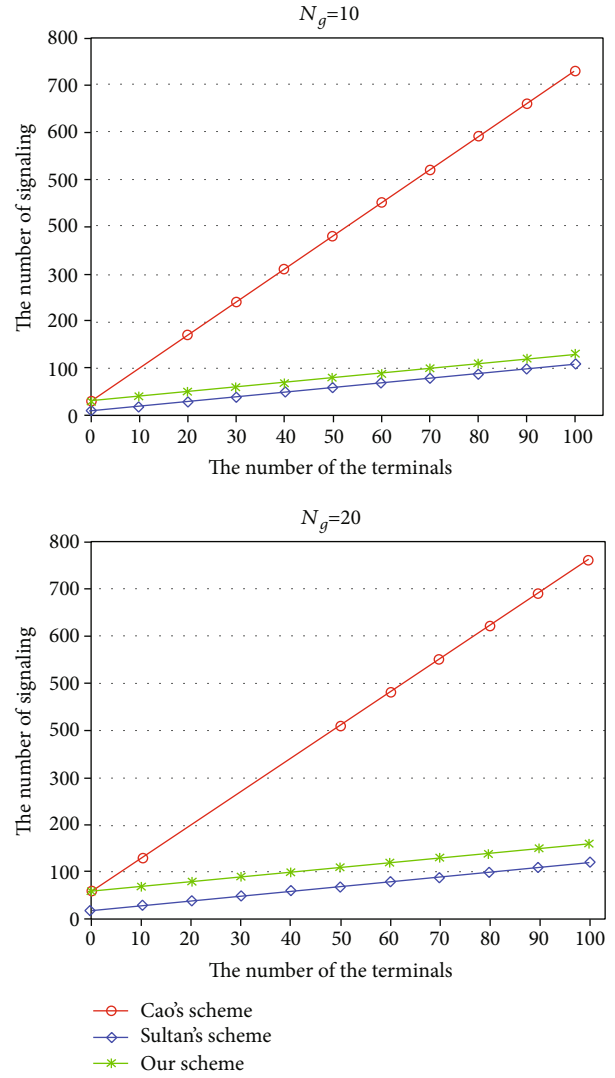

Figure 3: The comparison of signaling cost.

(3) Identity privacy protection: after the $\mathrm{IOTD}_{\mathrm{GID},i}$'s relevant information are encrypted in this scheme, it can protect the user's identity information from being leaked. According to the proposed scheme, we use AMF's public key to encrypt the $\mathrm{IOTD}_{\mathrm{GID},i}$ and GID. If an adversary wants to decrypt the information of interest, he must know the valid AMF private key. So, they cannot use the legal identity to further implement the replay attack

(4) Attack resistance: there are some attacks that can be resisted in our scheme, such as replay attacks,

Table 3: The symbol of notation.

Symbol	Definition
T_M	Time of a point multiplication
T_H	Time of a hash function operation
T_P	A pairing operation time

Table 4: The time required for the encryption operation.

UE	T_M	T_H	T_P
IOTD	4.312	0.514	31.812
AMF	1.048	0.036	8.671

modification attacks, impersonation attacks, eavesdropping, and man-in-middle attacks

(i) Replay attacks: since a random value is introduced to generate the signcryption in the construction of our scheme, which can resist replay attacks. In detail, we ensure the randomness of the message by selecting a random value v_i during the data transmission phase. Thus, the adversary cannot perform a replay attack without obtaining the value v_i

(ii) Modification attacks: in this proposal, a valid triple $(S, \{V_i, C_i\}_{1\le i\le I})$, S is the signature valid. We can check whether the message has been modified by the adversary through the formula $SP = V + \sum_{i\in I} h_{3,i}(X_i + R_i + h_{1,i}P_{\text{pub}})$

(iii) Impersonation attacks: when an adversary wants to send a forged message to AMF, it needs to be simulated as a legitimate device $\text{IOTD}_{\text{GID},i}$. At this time, AMF will test the formula $SP = V + \sum_{i\in I} h_{3,i}(X_i + R_i + h_{1,i}P_{\text{pub}})$, if it is established, it will pass the verification; otherwise, stop it

(iv) Man-in-the-middle attacks: our scheme can resist an attack such as an man-in-the-middle attacks. The prerequisite for the adversary to generate the correct signcryption or signature information is to know part of the private partial-key of AMF, which is related to the generation of the session key. And the generation of the session key requires the adversary to break the Computational Diffie-Hellman (CDH) problem. Specifically, in the data transmission and authentication encryption stage, we set multiple points(V_i, X_i, R_i, Z_i, etc.) on the elliptic curve in the content of the transmission message to ensure certain security. The adversary needs to break through the points we set on the curve based on CDH problem to obtain the corresponding private key and session key parameters

(v) Eavesdropping: no adversary can obtain the session key by eavesdropping. If an adversary can forge a signature or aggregate signature information, a private key needs to be forged to make entities AMF or $\text{IOTD}_{\text{GID},i}$ believe. In summary, the scheme is secure

Table 5: The computation overhead.

Protocol	IOTD_i	AMF
Cao's scheme	$T_H + 2T_M$	$2N_t(T_H + T_P)$
Sultan's scheme	$3T_H + 6T_M$	$N_t(T_H + 2T_M + 4T_P)$
Our scheme	$3T_H + 8T_M$	$(3N_t + 1)T_H + (5N_t + 1)T_M$

Based on the above analysis, the IMS in our scheme can resist the above-mentioned attacks to ensure the information security of the entire system. It prevents illegal users from entering the IMS by resisting replay attacks and impersonation attacks. And to ensure that the security of the information stored in the system by each entity in the IMS is not tampered with and eavesdropped through the other security features.

(5) Signaling Congestion Avoidance: we used the idea of certificateless signcryption technology to construct the scheme. A large number of IoT devices send access requirements to GLD, and GLD aggregates this information to generate messages. It can reduce the amount of signaling and effectively improving the efficiency of access authentication. The authentication process includes data transmission, which reduces the communication overhead of the scheme and reduces the pressure on the communication network

6. Performance Analysis

Compared with some similar schemes, this scheme has greater advantages in performance. In this part, we compare the signaling overhead, computing overhead, and communication overhead separately with Cao's scheme [24] and Sultan's scheme [27]. In Table 1, we describe the symbol definition where N_g and N_t represent the number of two different entities.

6.1. Signaling Overhead. In this section, we analyze our scheme, Cao's scheme [24], and Sultan's scheme [27]. And we take the number of signaling messages as a parameter.

In Cao's scheme, the communication between IOTD and AMF needs $7N_t + 3N_g$ signaling messages to realize authentication. In the scheme of Sultan, the communication between IOTD and AMF needs $N_t + N_g$ signaling messages to realize authentication. In this scheme, IoT devices and AMF achieve multiparty authentication need $N_t + 3N_g$ signaling messages. We can see the theoretical comparison results in Table 2.

In Cao's scheme, when the terminal communicates with the network, a great quantity access request messages can be integrated. Then, the aggregated message is sent to the network, which can be verified by AMF. After the

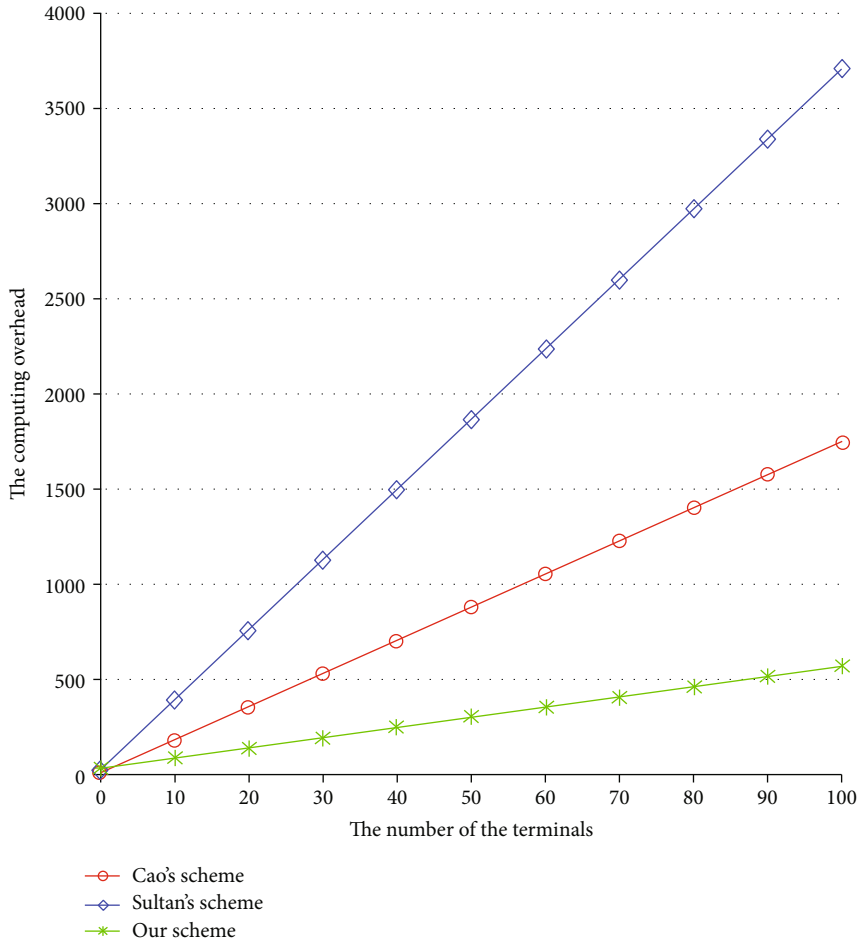

Figure 4: The comparison of computation cost.

authentication is successful, AMF sends messages to the terminal in broadcast mode. Due to the broadcast mechanism, Cao's scheme has higher signaling overhead compared with Sultan's scheme and our scheme. Based on aggregate signcryption technology, our scheme embeds data from different devices into authentication request messages. Then, they will be sent to AMF for authentication after aggregation by group leaders. In addition, the user terminal to authenticate the AMF generated signature authentication network through GLD. This method does not require each member to authenticate the message one by one, thereby greatly reducing the signaling overhead.

Figure 3 shows the change of the total number of signaling messages with the increasing number of terminal devices when $N_g = 10$ and $N_g = 20$, respectively. When the number of terminals increases from 1 to 100, the signaling cost in this scheme is similar to Sultan's scheme but is significantly better than Cao's scheme. It can be concluded that this scheme has good performance in signaling overhead.

6.2. Computational Overhead. In our scheme, we mainly consider three relatively time-consuming calculations (as shown in Table 3). T_M stands for dot multiplication operation, T_P stands for pair operation, and T_H stands for a hash operation. These calculations were tested on a laptop computer (Computer brand: Lenovo, processor: I5-3320 M 2.6 GHZ, memory: 4 G bytes, operating system: window7) and realized by calling the JPBC library. The running time of each operation is shown in Table 4.

Table 6: The communication overhead.

Protocol	Communication overhead
Cao's scheme	$(a+2+2c)N_t + (a+2)N_g$
Sultan's scheme	$N_t + N_g$
Our scheme	$aN_t + (a+2)N_g$

In Cao's scheme, the computational overhead of each IOTD and AMF is $T_H + 2T_M$ and $2N_t(T_H + T_P)$, respectively. In Sultan's scheme, the computational overhead of each IOTD and AMF are $3T_H + 6T_M$ and $N_t(T_H + 2T_M + 4T_P)$, respectively. In our proposed scheme, the computational overhead of each IOTD and AMF are $3T_H + 8T_M$ and $(3N_t + 1)T_H + (5N_t + 1)T_M$, respectively. We can see the computational overhead in each scheme from Table 5 and the relationship between them in Figure 4.

Due to the large number of pairing operations in Cao's scheme and Sultan's scheme, the computation cost of the two schemes is high. In Cao's scheme, the computational

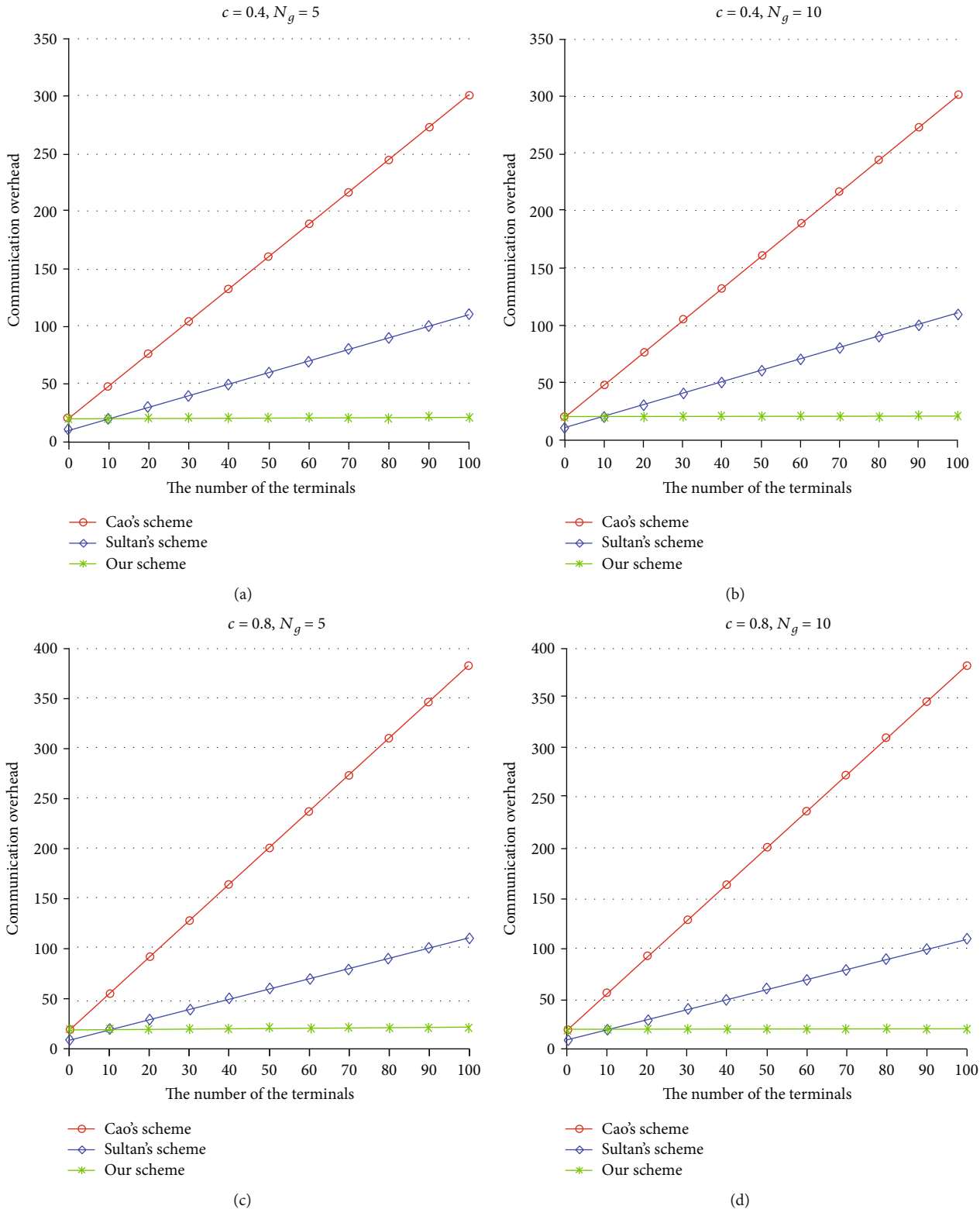

Figure 5: The comparison of communication cost.

cost of the protocol is the largest because it performs time-consuming mapping hash, bilinear pairing, and point multiplication. Our scheme realizes message aggregation authentication without bilinear pairing operation, so the computation cost of this scheme is less than that of the other two schemes. Figure 4 shows the comparison between the scheme in our scheme and the other two schemes. When the number of terminals increases from 0 to 100, the computational cost of the scheme in this chapter is significantly lower than that of the other two schemes.

6.3. Communication Overhead. We think that the transmission between AMF and $IOTD_i$ is a unit. There are a units between $IOTD_i$ and GLD, and c units are between eNB and $IOTD_i$. Since the distance between $IOTD_i$ and $IOTD_j$ is less than 100 meters, the cost of a units is much less than that of one unit. Due to different eNB locations, the distance between eNB and $IOTD_i$ is also various. Also, the distance between $IOTD_i$ and entities connected by wire is relatively fixed. In order to facilitate our analysis of the proposed scheme, we assume $a = 0.01$. Because of using the control plane to optimize the transmission mechanism, AKA scheme generates additional transmission overhead. During the establishment of the data holder, the consumption of AMF and $IOTD_i$ is two units. And the consumption of eNB and $IOTD_i$ transmission is $2c$ units.

After analysis, the communication cost of Cao's scheme is $(a + 2 + 2c)N_t + (a + 2)N_g$, that of Sultan is $N_t + N_g$, and that of our scheme is $aN_t + (a + 2)N_g$. In Table 6, the total communication overhead of Cao's scheme, Sultan's scheme, and our scheme are compared. Figure 5 shows the comparison of communication consumption between the scheme in this chapter and the other two schemes in four cases: $c = 0.4$, $N_g = 5$, $c = 0.4$, $N_g = 10$, $c = 0.8$, $N_g = 5$, $c = 0.8$, $N_g = 10$. It can be clearly seen from Figure 5 that when the number of user terminals increases from 0 to 100, the communication overhead of the scheme in this chapter is significantly lower than that of the other two schemes.

7. Conclusions and Future Work

In order to perform authentication and data transmission safely and efficiently in IMS, we propose an efficient and secure authentication for IoT device in information management systems. By screening the specific attributes of the device, an IOTD in the IoT group is selected as the group leader to perform message aggregation, signature, encryption, and transmission in our scheme. Therefore, while ensuring user identity privacy and data integrity, it greatly improves the efficiency of mutual authentication and data transmission between the user and the server in IMS. And it solves the large signaling overhead caused by multiple IoT devices simultaneously accessing the IMS, low authentication efficiency, and network congestion caused by processing multiple messages at the same time. Then, security analysis shows that the protocol can resist various malicious attacks. Performance analysis also shows that this scheme is effective in terms of signaling overhead, computing overhead, and communication overhead. In future research, it will be interesting to design a secure, efficient, and meet the needs of more intelligent scenarios in a IoT device authentication scheme.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors have declared that no conflict of interest exists.

Acknowledgments

This work is supported by the National Key R&D Program of China (2017YFB0802000), the Key Research and Development Program of Shaanxi (2019KW-053, 2020ZDLGY08-04), the Innovation Capability Support Program of Shaanxi (2020KJXX-052), Guangxi Cooperative Innovation Center of Cloud Computing and Big Data (No. YD1903), and the Basic Research Program of Qinghai Province (No. 2020-ZJ-701).

References

[1] K. B. Jalbani, A. H. Jalbani, and S. S. Soomro, *IoT Security: To Secure IoT Devices With Two-Factor Authentication by Using a Secure Protocol*, Industrial Internet of Things and Cyber-Physical Systems: Transforming the Conventional to Digital, 2020.

[2] R. Arshad and N. Ikram, "Elliptic curve cryptography based mutual authentication scheme for session initiation protocol," *Multimedia Tools and Applications*, vol. 66, no. 2, pp. 165–178, 2013.

[3] S. K. Hafizul Islam and G. P. Biswas, "Design of improved password authentication and update scheme based on elliptic curve cryptography," *Mathematical and Computer Modelling*, vol. 57, no. 11-12, pp. 2703–2717, 2013.

[4] M. Hou, T. Kang, and L. Guo, "A blockchain based architecture for IoT data sharing system," in *2020 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, Austin, TX, USA, March 2020.

[5] S. Mandal, B. Bera, A. Kunar, K. Kwang, and Y. Park, "Certificateless-signcryption-based three-factor user access control scheme for IoT environment," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 1–1, 2020.

[6] Huawei Technologies Co, "5G Opening Up New Business Opportunities.," White Paper, 2016.

[7] 3GPP, "Study on The Security Aspects of the Next Generation System," Technical Report, 2017.

[8] 5G PPP, "5G PPP Phase 1 Security Landscape," 2017.

[9] NGMN, "5G Security Recommendations (Networking Slicing, Mobile Edge Computing)," White Paper, 2016.

[10] Nokia, "Security Challenge and Opportunities for 5G Mobile Networks," White Paper, 2017.

[11] D. Wang, J. Shen, J. Liu, and K. K. R. Choo, "Rethinking authentication on smart mobile devices," *Wireless Communications and Mobile Computing*, vol. 2018, Article ID 7079037, 4 pages, 2018.

[12] T.-Y. Teh, Y.-S. Lee, Z.-Y. Cheah, and J.-J. Chin, "IBI-mobile authentication: a prototype to facilitate access control using identity-based identification on mobile smart devices," *Wireless Personal Communications*, vol. 94, no. 1, pp. 127–144, 2017.

[13] W. I. Khedr, K. M. Hosny, M. M. Khashaba, and F. A. Amer, "Prediction-based secured handover authentication for mobile cloud computing," *Wireless Networks*, vol. 26, no. 6, pp. 4657–4675, 2020.

[14] A. P. G. Lopes and P. R. L. Gondim, "Group authentication protocol based on aggregated signatures for d2d communication," *Computer Networks*, vol. 178, article 107192, 2020.

[15] H. Yang, Y. Wu, J. Zhang, H. Zheng, Y. Ji, and Y. Lee, "Blockonet: blockchain-based trusted cloud radio over optical fiber network for 5G fronthaul," in *2018 Optical Fiber Communications Conference and Exposition (OFC)*, pp. 1–3, San Diego, CA, USA, March 2018.

[16] H. Yang, Y. Li, S. Guo, J. Ding, Y. Lee, and J. Zhang, "Distributed blockchain-based trusted control with multi-controller collaboration for software defined data center optical networks in 5G and beyond," in *2019 Optical Fiber Communications Conference and Exhibition (OFC)*, San Diego, CA, USA, March 2019.

[17] Y. Zhang, R. H. Deng, E. Bertino, and D. Zheng, "Robust and universal seamless handover authentication in 5G HetNets," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 2, pp. 858–874, 2021.

[18] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008, http://bitcoin.org/bitcoin.pdf.

[19] Y. Chen, J. Wang, K. Chi, and C. Tseng, "Group-based authentication and key agreement," *Wireless Personal Communications*, vol. 62, no. 4, pp. 965–979, 2012.

[20] S. Basudan, "LEGA: a lightweight and efficient group authentication protocol for massive machine type communication in 5G networks," *Journal of Communications and Information Networks*, vol. 5, no. 4, pp. 457–466, 2020.

[21] Y. Aydin, G. Karabulut, and H. Yanikomeroglu, "A flexible and lightweight group authentication scheme," *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 10277–10287, 2020.

[22] C. Lai, H. Li, R. Lu, and X. S. Shen, "Se-aka: a secure and efficient group authentication and key agreement protocol for LTE networks," *Computer Networks*, vol. 57, no. 17, pp. 3492–3510, 2013.

[23] R. Jiang, C. Lai, J. Luo, X. Wang, and H. Wang, "EAP-based group authentication and key agreement protocol for machine-type communications," *International Journal of Distributed Sensor Networks*, vol. 11, 318 pages, 2013.

[24] J. Cao, M. Ma, and H. Li, "Gbaam: group-based access authentication for MTC in LTE networks," *Security and Communication Networks*, vol. 8, no. 17, pp. 3282–3299, 2015.

[25] C. Lai, H. Li, R. Lu, R. Jiang, and X. Shen, "Lgth: a lightweight group authentication protocol for machine-type communication in LTE networks," in *2013 IEEE Global Communications Conference (GLOBECOM)*, pp. 832–837, Atlanta, GA, USA, December 2013.

[26] J. Li, M. Wen, and T. Zhang, "Group-based authentication and key agreement with dynamic policy updating for MTC in LTE-a networks," *IEEE Internet of Things Journal*, vol. 3, no. 3, pp. 408–417, 2016.

[27] S. Basudan, X. Lin, and K. Sankaranarayanan, "A privacy-preserving vehicular crowdsensing-based road surface condition monitoring system using fog computing," *IEEE Internet of Things Journal*, vol. 4, no. 3, pp. 772–782, 2017.

[28] Y. Zhang, F. Ren, A. Wu, T. Zhang, J. Cao, and D. Zheng, "Certificateless multi-party authenticated encryption for NB-IoT terminals in 5G networks," *IEEE Access*, vol. 7, pp. 114721–114730, 2019.

[29] S. Behrad, E. Bertin, S. Tuffin, and N. Crespi, "A new scalable authentication and access control mechanism for 5G-based IoT," *Future Generation Computer Systems*, vol. 108, pp. 46–61, 2020.

[30] B. Seok, J. Sicato, T. Erzhena, C. Xuan, and J. Park, "Secure D2D communication for 5G IoT network based on lightweight cryptography," *Applied Sciences*, vol. 10, no. 1, p. 217, 2019.

[31] J. Sanchez-Gomez, D. Garcia-Carrillo, R. Marin-Perez, A. Skarmeta, and A. Skarmeta, "Secure authentication and credential establishment in narrowband IoT and 5G," *Sensors*, vol. 20, no. 3, p. 882, 2020.