IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received November 5, 2019, accepted December 1, 2019, date of publication December 25, 2019, date of current version January 15, 2020.

Digital Object Identifier 10.1109/ACCESS.2019.2962247

A Smart Collaborative Authentication Framework for Multi-Dimensional Fine-Grained Control

ZHENGYANG AI[1], YING LIU[1], LIU CHANG[2], FUHONG LIN[3], AND FEI SONG[1]

[1]School of Electronic and Information Engineering, Beijing Jiaotong University, Beijing 100044, China
[2]Network Technology Research Institute, China Unicom, Beijing 100044, China
[3]School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing 100083, China

Corresponding author: Fei Song (fsong@bjtu.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61602034, and in part by the Joint Foundation of China University of Petroleum-Beijing at Karamay.

ABSTRACT The emergence of the 5G network has brought broad prospects for the massive terminal access and ubiquitous Internet of Things (IoTs). Potential attacking opportunities triggered by this progress are severely impacting the security fortress of current networks, especially in the edge access part. However, due to the unitary protection and inferior isolation, available security schemes are incapable of effectively eliminating these hidden perils. Motivated by these facts, we propose a Multi-dimensional Fine-grained Control (MFC) framework to strengthen safety and reliability in Radio Access Networks (RANs). First, we comprehensively survey and summarize the existing security schemes to grasp respective effects and limitations. Second, the MFC framework is established to describe the model structure and implementation processes. An identifier mapping mechanism is designed to achieve network isolation. We perform the security analysis of MFC by theoretically comparing diversified policies. Third, an integrated set of the authentication prototype system is created with wireless environment parameters settings. Specific verification scenarios are illustrated. Finally, we test the performances of the MFC framework. Validation results demonstrate that the proposed scheme can accomplish reliable security control at the access side. Comparing to multiple schemes, the performances, in terms of time and concurrency, are optimized. Therefore, the MFC framework is feasible for applications in 5G or IoT.

INDEX TERMS Edge access control, multi-dimensional authentication, unique user identifier, bidirectional control.

I. INTRODUCTION

As the 5G network continues to mature, various technologies, such as Multi-access Edge Computing (MEC), Content Delivery Network (CDN), virtual reality, and multimedia, have been developed rapidly. The network is also continually showing the characteristics of diverse users, heterogeneous structures, sophisticated services, and massive data. However, network security is facing daunting challenges and tribulations brought by the development of the IT industry, which also provides an opportunity for attackers. According to the Cyber Attack Trends: 2019 MID-YEAR Report [1], multiple cyber threats have grown in the first half of this year, including supply chain attacks, email spoofing attacks, cloud attacks, and mobile attacks. In terms of data breaches, the hacking forum Collection ♯1 leaked 770 million email addresses and 21 million passwords. The developers of the Facebook third-party app leaked 500 million user records. The AMCA leaks affected 20 million patients, and there are countless such cases. Also, the Radware released the latest "2018-2019 Global Application and Network Security Report," [2] saying that the initial cost of cyberattacks increased by 52% per year, 93% of respondents have been hacked in the past 12 months, and one-third of companies are attacked every week by cyber attacks. Faced with such a severe network environment, we urgently need to optimize the network system to ensure the security of privacy and property.

As the first valve of network security, the network access side forms a connecting link between the preceding and following in data transmission, and attackers directly threaten it. Therefore, it is critical to quickly detect and block threats at the edge of the network, keeping malicious data out of the core of the network. However, the original design of the

The associate editor coordinating the review of this manuscript and approving it for publication was Antonio Skarmeta Gómez.

Internet was mainly for data service transmission [3]. It is a scale-free network with a power-law structure. This design makes the Internet vulnerable to malicious attacks and security loopholes emerge one after another. Besides, to ensure the integrity, availability, confidentiality, and privacy of network data, a large number of researchers have proposed a variety of solutions [4], i.e., 1) Encryption/decryption techniques, including various digital signatures [5], public key encryption [6], [7], digital watermarking techniques [8]. 2) Access control technologies, including firewall technology, Discretionary Access Control (DAC), Mandatory Access Control (MAC) [9], Role-Based Access Control (RBAC) [10], [11], Attribute-Based Access Control (ABAC) [12], etc. 3) Security monitoring technology, including intrusion detection and prevention systems [13], [14], biometrics [15], honeypot technology [16], information filtering, and more. Although technologies are emerging in an endless stream, they are generally limited by the following deficiencies.

(1) Single protection measures: The rapid development of novel technologies inevitably leads to tremendous changes in the network, e.g., service types, users groups, and network scope. At present, most of the studies intently focus on a certain aspect of security, which is challenging to cope with the complex and changing network environment. Security challenges should be addressed from multiple perspectives as much as possible.

(2) Inferior network isolation: Due to the limitations of resource and location binding, control and data binding, and user-network binding on the original design of the Internet, it is difficult for existing networks to adapt to dynamic and complex security requirements. In particular, the edge network is poorly isolated from the core network, which puts much pressure on the core network.

(3) Lack of source and destination two-way control: At present, most access control measures only judge the data source, and do not adequately consider the data type and destination address. This process easily exposes network vulnerabilities and increases insecurity. The bilateral control not only ensures the legitimacy of the source but also guarantees the validity of the destination address.

(4) Lack of user uniqueness and level control: The design of the Internet assumes the trust of the terminal node as a precondition. The terminal node can access the network as long as the correct IP address is configured, which lacks the effective user access control mechanism. Most current solutions cannot locate the user's access location and unique identifier, which is challenging for administrators to track users' behaviours dynamically.

Motivated by the above considerations, we propose a Multi-dimensional Fine-grained Control (MFC) framework for Radio Access Networks (RANs). The framework introduces the User Type Approval (UTA) network access device with fingerprint unlocking function. This device embeds a unique Access IDentifier (AID) which is allocated for users based on fine-grained attributes, and each AID corresponds to a user level. Also, we devise a bidirectional control mechanism of source and destination at the edge side. An identifier mapping mechanism is proposed for network identifier transformation to realize the isolation mechanism of the edge side and core network. The authentication server registers and assigns different-level UTA devices for uses, according to their User Information (UI). The system implements the user's authentication function by controlling the user's AID authority, fingerprint characteristics, and access rights. We first investigate the existing security solutions and analyze them separately from three aspects. Based on their questions, we introduce the basic framework of the proposed framework, including fundamental ideas, system models, workflow, and security analysis. To further prove the effectiveness of the scheme, we design a prototype system, then give the system structure and deployment. Finally, the superiority of our program is verified. In this paper, our main contributions can be summarized as follows.

- We propose a high-security multi-dimensional fine-grained identifier authentication framework, which integrates a variety of security measures and has the characteristics of fine-grained control of user identifier, resistance to security attacks. Also, the framework guarantees that users are unique and legitimate, realizes the separation of access and core network, meets dynamic monitoring needs, and optimizes authentication delay.
- A source and destination bidirectional control mechanism is proposed and incorporated into the framework, which ensures both source availability and destination validity.
- We build a prototype system for the proposed scheme, which breaks the currently rigescent network, modifies the authentication process, and isolates the access side from the network side, aiming to ensure the internal security of the network. On this basis, we verify the proposed solution.
- We carry out sufficient theoretical analysis and systematic verification. The final results prove that the proposed scheme can achieve unified access control management for access users, optimize authentication delay compared with other authentication schemes, and support the high concurrency performance, which lays a solid foundation for further researches.

The rest of this paper is organized as follows: In Second II, we introduce existing researches from three aspects and analyze their advantages and disadvantages. In Second III, we present an overview of the proposed solution, including basic ideas, system model, and workflow. Also, we conduct a security analysis of various schemes. In Second IV, we establish a prototype system and describe the system configuration, structure, and deployment. In Second V, the verification results are provided. Finally, we conclude and give a future perspective in Second VI.

II. RELATED WORK

With the continuous development of information networks, cyberattacks are changing with each passing day, and have

evolved from small-scale attacks to large-scale, distributed, and diverse means. For various security threats, network protection technologies have gradually evolved from passive methods to active monitoring. There are already a large number of security studies [17], [18], and they mainly involve three aspects, namely encryption/decryption technology, access control technology, and security monitoring and surveillance technology.

A. ENCRYPTION/DECRYPTION TECHNOLOGY

This technology secretly exchanges stored or transmitted information for data confidentiality and is mainly classified into file encryption, password encryption, and transmission encryption.

Currently, searchable encryption schemes are for server access. Due to the user's unrestricted searchability, Yin *et al.* [19] proposed an encryption search scheme based on attribute control, which can determine whether there is search permission according to user attributes and achieve fine-grained access control. However, the authors only gave the performance results, and the functional characteristics were lacking. Also based on attribute policies, the paper [20] designed an updateable attribute-based encryption scheme by adding a fixed identifier to the encryption key. The difference is that this method was used for traceability and revocability. Unlike the paper [20], Huang *et al.* [21] presented a deniable authentication encryption scheme for privacy protection by making it impossible for the receiver to provide message proof. The authors considered some awkward conversations over the internet, including doctor-patient medical conversations or lawyer-criminal discussions.

Similarly, the paper [22] proposed an improved mixed authentication scheme to protect the privacy of patients in the modern health-care area. This method combined a password, smart card, and biometric feature to ensure network security in many ways. However, the scheme lacked an evaluation of validation time. A multi-level encoding and encrypted-hash-based digital signature were presented in [23], aiming to resist the destruction of intellectual property in the consumer electronics system. This scheme achieved stronger robustness and less storage hardware. For authenticating big data and software scenarios, the digital signature generation process is time-consuming. Therefore, Chen *et al.* [24] devised a lattice-based incremental signature scheme which could produce signatures quickly. However, there is not much concern about improving safety.

Although encryption/decryption technologies can protect user data from eavesdropping and tampering, it only focuses on service data without the ability to identify abnormal user behaviours. For the zombie host, a single encryption method appears powerless.

B. ACCESS CONTROL TECHNOLOGY

Access control technologies set the user's access restrictions at the network access side. Based on the predefined feature rules, it limits the request for resource access. It is mainly divided into identity information verification and firewall technology.

In terms of the attribute-based control, the authors [25] proposed a hierarchical access control method by modifying the hierarchical attribute-based encryption and structure. This method ensured data confidentiality and user legitimacy in the mobile cloud computing system. In [26], a distributed attribute-based access control system was presented, which provided a distributed policy management to allow users to set up policies for the Internet of Things (IoT) devices. This method ensured confidentiality and prevented network attacks at the edge of networks. Also, in IoT networks, Ding *et al.* [27] proposed a new access control scheme by using Blockchain technology. Attributes of users were recorded to avoid single node failure and data tampering. In [10] and [28], they all considered cloud storage security. The former tended to introduce the concept of a trusted system based on Role-Based Access Control (RBAC) to improve network security. While the latter tended to solve the problem of access collaboration. An attribute-based collaborative access control scheme was proposed to coordinate the access of users with different attributes and guarantee the legitimacy of users.

Similar to [10], an RBAC-based access control scheme was devised in [11], which combined smart contracts and Blockchain technology to realize a challenge-response authentication protocol. This platform achieved secure, flexible, and adaptive access for users. In [29], the authors proposed a novel cryptographic authentication scheme, named CCA2-PV-R-LU-MA-ABE in fog computing. The creation of private keys depended on the geographical locations and functions of nodes. Besides, the attributes of nodes can be denoted by any strings, and only valid ciphertext can be stored or transmitted. Lin *et al.* [30] presented a local authentication access control scheme, which enabled authorized users to secure access to M2M devices. In this scheme, the M2M devices can locally verify the rights and privileges of users. Also, they can transfer heavy computation to the user equipment. To reduce computation overhead and delay in Information-Centric Networking (ICN) authentication, a secure, efficient, and accountable edge access control scheme was designed by adopting group signature and hash chain techniques [31]. This framework not only reduced overhead but also provided service accountability. In [32], the authors considered not only a single authentication method, but a two-factor scheme, including password and smart card. On this basis, a card reader verification process is added to the authentication scheme to prevent smart cards from being attacked.

For access control technologies, whether role-based or attribute-based, the purpose of these schemes is to control the initiator of service requests to access a particular type of service. But there is little valid identification of the destination end, which increases network redundancy and lacks judgment on the validity of access data.

C. SECURITY MONITORING AND SURVEILLANCE TECHNOLOGY

This technology monitors the network data stream in real-time through hardware or software, then compares it with the characteristics of the abnormal data labelled by the system. Once an attack is detected, it responds according to the actions defined by the rule.

The emergence of machine learning technologies undoubtedly promotes the development of network surveillance. In [33] and [34], both of them adopted deep learning algorithms to detect network traffic. One was applied in SDN networks, and the other was deployed in the 5G network. The purpose of them was to ensure network reliability and optimize resource consumption. Reshan *et al.* [35] ensured communication security between Body Area Network (BAN) devices by combining biological traits and time-varying physiological signal characteristics. These devices contained a large amount of user's private information, and they authenticate to each other by multiple biometric and physiological features to discover anomalies.

A self-healing neuro-fuzzy anomaly detection approach was proposed to achieve the detection, recovery, and removal of horizontal anomalies in social networks [36]. This scheme was implemented on multiple paradigms and datasets with high detection accuracy and abnormal filtering rate. To reduce the false alarm rate of the detection system, Meng *et al.* [37] designed a hierarchical framework to mine high-threat alerts from a large number of alarm logs, to provide available information for the management system to modify the judgment policy. In [38], the authors developed a dynamic distributed honeypot and combined it with the Blockchain platform, to discover attacks and resist anti-honeypot technology in time. This scheme achieved high reliability, high security, and low response time.

For security monitoring technologies, the validity of data and tagged features is critical to safety protection. However, this technique is limited by samples and unknown attacks, and there are cases of missed and false positives. Besides, for the existing complex network environment, a single security monitoring strategy has been challenging to meet the high-security needs.

Therefore, through the analysis and sorting of the present works, we find that most of the schemes are faced with such problems as a single technology, difficult positioning of users, poor isolation between edges and core. It is difficult to deal with the network environment with diverse subjects and objects [39], diversified control basis and complex and changeable control strategies. Faced with a large number of security threats, how to effectively maintain the security of the network has become a crucial problem to be solved.

III. MFC FRAMEWORK

Given the shortcomings of existing security solutions, we propose a novel authentication framework that optimizes the authentication delay, resists security attacks and provides user-level services. The framework realizes the separation of the access network from the core network. It assigns a level to the user, which facilitates the user's fine-grained management and on-demand services. Also, it introduces the unique user identifier in the protocol design for authentication and exploits user password information. In the implementation path, a smart access device UTA is added, and fingerprint identification is required. Besides, we design a two-way data verification mechanism on the edge node. In this section, we first introduce the MFC model and describe the module components. Second, the framework's workflow is given in detail. Finally, we conduct a security analysis.

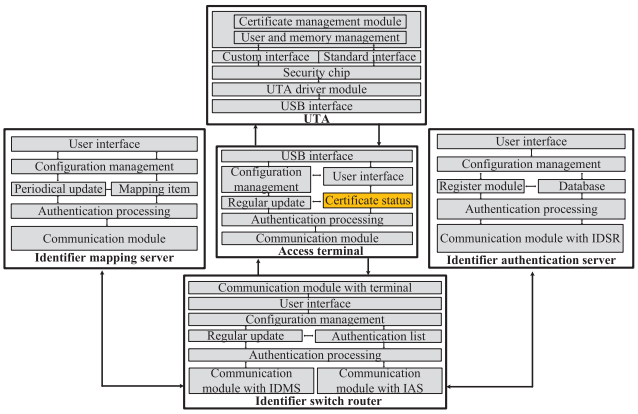


FIGURE 1. The module components of MFC.

A. MFC MODEL

In the MFC framework, there are mainly five modules related to the proposed framework, namely UTA device, IDentifier Mapping Server (IDMS), access terminal, Identifier Authentication Server (IAS) and IDentity Switch Router (IDSR), as shown in Figure 1.

1) UTA MODULE

The UTA module is a user access medium, which is composed of hardware, firmware, driver, and upper-layer software. Also, it includes a fingerprint unlocking function. The digital certificate and AID identifier are stored in the encrypted UTA device for identity authentication.

2) ACCESS TERMINAL

It is a device for users to access a network, including login and registration interfaces. There are a variety of terminal categories, including fixed and mobile devices. However, the standard modules include UTA interface, configuration management interface module, and user interface.

3) IDMS MODULE

IDMS module is used to store mapping entries from the access side to the core network segment, including IP address, AID, Router IDentifier (RID), and rights. The AID is used to locate the user on the access side, while the RID is used to dynamically transmit the user information in the core

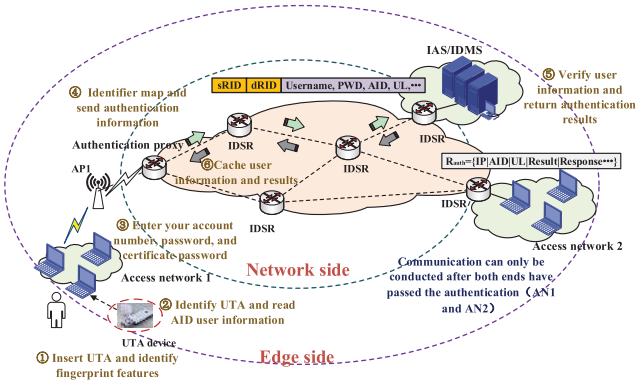


FIGURE 2. The system topology of MFC.

network to achieve separation of the access and core parts. User information is hard to be leaked in the core network.

4) IDSR MODULE

IDSR module is located at the boundary between the core network and the access network. In addition to the basic forwarding function, IDSR not only implements pre-authentication of the system but also provides mapping service functions, that is, AID to RID conversion. Besides, the proposed bidirectional control mechanism is deployed here.

5) IAS MODULE

It is one of the core parts of the MFC framework, which is used to store information items of legitimate users, including registered User Information (UI), AID information corresponding to UTA, and user rights.

The above five modules are the leading network element entities of the framework, where the terminal is located on the user access side, and the IAS and IDMS are located on the network space side. The IDSR is a handover point between the user space and the network space and implements a separate mapping between the AID and RID. The specific topology is shown in Figure 2. After users access the network, the MFC can control the rights and behaviours of users to ensure the security and reliability of the network operation.

B. IMPLEMENTATION PROCESS

The MFC framework contains two processes: pre-registration and authentication at the time of use. That is, if a user wants to access the network and obtain services, he must register individual information in the management system. Then the user is assigned the appropriate level and given a UTA device with a unique identifier. When the user accesses the network, the network authenticates the user according to the information registered by the user in advance, thereby achieving reasonable control of the user rights. The implementation process is shown in Figure 3.

1) USER REGISTRATION AND UTA ACQUISITION

MFC framework allows different user groups and various types of devices to access the network. However, before users enter the network, they need to register and provide the fine-grained attributes of the user, such as the user's name, gender, position, address, and telephone number. In this paper, we abstract these basic properties to A_i, then all attributes of the user are represented as:

$$P \subseteq \{A_i : 1 \leq i \leq n\} \tag{1}$$

In the IAS server, in addition to the individual attributes P for user registration, there is also authentication information (username, password, certificatepwd, etc.), which is collectively referred to as UI. In the formula (1), i is the ith attribute value, and n represents the number of attributes. The function $I_i(A_i)$ is defined as the formatting function of the ith attribute, which satisfies:

$$I(A) = \sum_{i=1}^{n} I_i(A_i) \tag{2}$$

In the MFC framework, the AID identifier containing user levels is generated based on user attributes. According to equations (1) and (2), it can be expressed as:

$$AID = I(P) = \sum_{i=1}^{m} I_i(p_i) \tag{3}$$

where $p_i \in P$, $1 \leq m \leq n$, and m stands for the number of abstract attributes. After the user registers this information in the system, the authentication server assigns the UTA device containing AID to the user and determine the user level. The stored information can be expressed as:

$$Info_{reg} = (UI, AID, userlevel) \tag{4}$$

After completing the above application process, the user can get access to the network device and attempt to complete the subsequent authentication process. The specific application process is shown in Figure 4.

2) USER AUTHENTICATION PROCESS

To establish a mutual-trust network environment between the user and the network, the user and the network must also complete the following authentication process. Otherwise, both parties suppose that the other party is false or abnormal, and cannot conduct any subsequent data communication.

Step 1: After the UTA device is inserted into a terminal and the fingerprint unlocks successfully, the user terminal initiates a request $R_{authque}$ to the network, where the authentication packet field includes: $R_{authque} = \{IP|username|pwd|AID|certificatepwd|challenge|\ldots\}$.

Step 2: After receiving the data packet $R_{authque}$, the IDSR first determines the service type, and if the data is a management data (DHCP and authentication data), it passes by default. Otherwise, the data is service data. The IDSR determines whether the source IP and AID information are local. If not, access users are illegal. Then a redirect is performed for authentication. 3. If it exists, check if the destination address exists in the IDMS. If the destination address is valid, perform identifier mapping, and enter the core network.

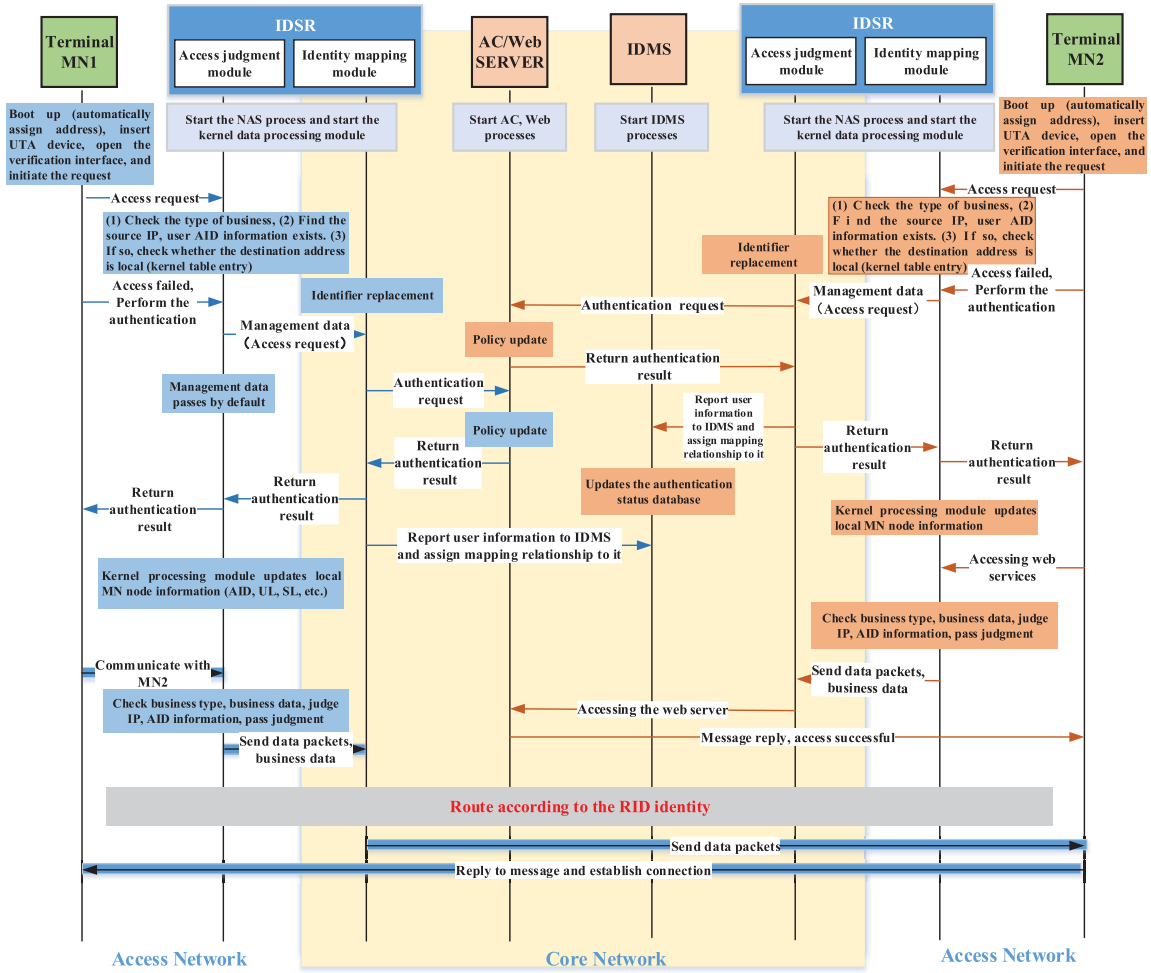


FIGURE 3. The implementation process of MFC.

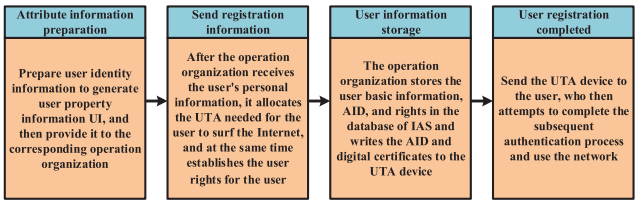


FIGURE 4. The user registration process of MFC.

Step 3: If the data is a management data, the data is sent directly to the IAS.

Step 4: After receiving the data packet $R_{authque}$, the IAS checks whether the user name, password, certification password, and AID information are consistent with the information in IAS. If the user is valid, the IAS returns the data packet $F_{authque} = \{IP|AID|response|userlevel|\ldots\}$ to the IDSR as the authentication result, otherwise, discards the data.

Step 5: After the IDSR receives the message, it checks the authentication result. If the user is legal, it assigns the corresponding RID information and caches the mapping entry in the IDSR. The cache entry includes: $\{IP|AID|RID|userlevel\}$. Besides, the AID and IP information passed through the authentication are cached in the local authentication table. Finally, the IDSR returns the data to the client.

Step 6: After the user receives the result, business communication can be conducted.

3) BUSINESS COMMUNICATION PROCESS

In Step 2 above, when the data is judged as a business data, and the access user is legal, the mapping search of IDMS can be carried out. After the mapping from AID to RID is executed, normal user communication can be realized.

Once the above process is completed, the network achieves the communication of the business. The pseudocode of the whole process is illustrated in Figure 5. In the MFC framework, the related cache information and mapping information disappears when the user unplugs his UTA from the device. Thus, cached information can be dynamically updated and maintained.

C. SECURITY ANALYSIS

In this section, we analyze the security features of the framework from three aspects.

```
Implementation process of MFC framework
1: Init UI, AID, RID, UTA, IAS, IDMS, and IDSR;
2: the user registers personal information UI to the server;
3: based on the UI, the server assigns a user level and issues UTA;
4: insert UTA device and fingerprint to unlock;
5: while the unlock works
6:    the terminal initiates a request R_authque (management or business);
7:     IDSR receives the data and checks it;
8:    if the data is a management data then
9:        it passes by default and is sent directly to the IAS;
10:       IAS receives the data and verifies it;
11:       if the AID, username, password, and so on are correct then
12:          the user is legal and return the authentication result;
13:          IDSR assigns mapping entries, and caches user information;
14:          the terminal receives the result and starts a service;
15:       else
16:          the user is illegal and the service is terminated ;
17:       end if
18:   else
19:       the data is a business data and perform packet checking;
20:       if the source IP and AID are in the local list then
21:          if the destination IP exits in the IDMS then
22:             perform identity mapping from AID to RID;
23:             the data enters the core network and communication with
24:             other users or servers is permitted;
25:          else
26:             discarding the data;
27:          end if
28:       else
29:          user is unauthenticated and redirected to the authentication
30:          step 10;
31:       end if
32:   end if
33: end while
34:    the user is illegal and barred from the network
35: finished
```

FIGURE 5. The pseudocode of the whole process.

1) SECURE CONTROLLABLE ACCESS CAPABILITY

The proposed framework involves multiple-dimensional protection measures such as using unique identification authentication, access device usage, biometrics, and a bidirectional control mechanism. It realizes the unique confirmation of the access user, traceability of user location, and hierarchical control. The user implements access control through individual identity authentication to achieve the user's authorized access by comparing the identifier, biometric features, and username. At the same time, in the design of MFC framework, when there is a network authentication terminal, the terminal needs to send an authentication parameter information, while when the terminal authenticates the network, the network needs to answer the challenge. The setting of these two processes ensures mutual trust between the two parties, thus achieving secure and controllable access.

2) ENDOGENOUS SECURITY AND ATTACK DEFENSE

The proposed framework adopts the idea of user information and location separation. The user on the access side routes through the unique AID identifier. When accessing the core network, the IDSR mapping relationship is adopted, i.e., the AID-RID conversion process. In the core network, the data packet is routed through the RID identifier. The attacker can only learn the user data location and cannot obtain the individual information. Besides, data can be routed on-demand in the core network, according to different levels of users. The idea that the user is separated from the network and forwards data based on the route identifier prevents attackers from learning the internal information of the network, and it is difficult to attack the core network, thereby realizing the functions of endogenous security and attack defence.

3) DIFFERENTIATED-SERVICE SECURITY CAPABILITY

In the user authentication process, the system assigns an AID identifier to the user according to the UI information. The AID information covers the user level, and the AID and the RID implement a mapping relationship. In the core network, different link resources can be allocated according to the RID information. This paper only covers the isolation of the network domain and does not involve the identifier routing control system of the core network. However, the dynamic update forwarding in the future can realize the dynamic transmission of data and the flexible control of the data. Finally, low-priority data is transmitted according to the default route, and high-priority nodes are inserted into the queue. Besides, the system can control different-level users access to services, which realizes the function of differentiated-service capability.

Through the above analysis, we compare our scheme with other schemes, and the comparison results are summarized in Table 1. As shown in the table, our scheme provides a more comprehensive security measure, comparing our scheme from multiple dimensions. Therefore, the proposed scheme is superior to other schemes in terms of safety function comparison.

IV. PROTOTYPE SYSTEM ESTABLISHMENT

To verify the validity of the proposed framework, we build a prototype system in the wireless access scenario. Both the C and Java programming are involved in modifying kernel code and protocol primitives [45]. In this section, we describe the system composition, deployment environment, and verification scenarios.

A. SYSTEM COMPOSITION

The prototype system of the MFC framework is shown in Figure 6, which consists of hardware devices and software protocols. The hardware equipment mainly includes five General Switch Routers (GSR) in the core network, four IDSRs for the access network, two control center servers, four user terminals, four UTA access devices, and four AP access nodes. In this prototype system, we use mobile laptops as access terminals.

The hardware device of IDSRs in the prototype system uses a universal dual-board card, in which one board is used to implement identifier conversion and forwarding. The proposed framework is compatible with existing IPv4/6 protocols, while the other board is responsible for access control. The software running environment of terminals is Windows7/Linux, and the setting of other devices is Linux. The specific list is shown in Table 2.

TABLE 1. The performance comparisons of various schemes.

Property / Schemes	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}	P_{13}	P_{14}	P_{15}	P_{16}
Wang et al. [42]	N	Y	N	N	Y	N	Y	Y	N	Y	Y	Two	Y	Y	N	Y
Xiong et al. [34]	N	Y	Y	N	Y	Y	Y	Y	N	Y	Y	Two	Y	Y	N	N
Chen et al. [22]	Y	Y	Y	N	Y	Y	Y	Y	N	N	Y	Three	Y	Y	Y	Y
Maitra et al. [43]	N	Y	Y	N	Y	N	Y	Y	N	Y	Y	Two	Y	Y	Y	N
Xie et al. [44]	N	Y	N	N	Y	N	Y	N	N	Y	N	Two	Y	Y	Y	N
Li et al. [45]	Y	Y	Y	N	Y	Y	Y	Y	N	Y	Y	Three	Y	Y	N	N
Park et al. [46]	Y	Y	N	N	Y	Y	Y	Y	N	Y	N	Two	Y	Y	Y	N
MFC	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Multi-dimension	Y	Y	Y	Y

[1] **Note**: Y: Have this property, N: No such property, P_1: Resistance against biometric recognition attacks, P_2: Resistance against replay attacks, P_3: Resistance against impersonation attacks, P_4: Realize the separation of the edge and core network, P_5: Resistance against password guessing attacks, P_6: Resistance against malicious smart device reader attacks, P_7: Resistance against man-in-middle attacks, P_8: Resistance against privileged insider attacks, P_9: Achieve bidirectional address control, P_{10}: Achieve mutual authentication, P_{11}: Achieve user anonymity, P_{12}: Security factor, P_{13}: Resistance against stolen smart device attacks, P_{14}: Resistance against forgery attacks, P_{15}: Achieve user uniqueness and traceability, P_{16}: Achieve fine-grained control of multi-level users.

TABLE 2. The node list of prototype system.

Num	Equipments classification	Hardware environment	Software environment	Count
1	GSR	Universal dual boards	Linux	5
2	IDSR	Universal dual boards	Linux	4
3	IDMS server	Universal server	Linux	1
4	IAS server	Universal server	Linux	1
5	Access teminal	Mobile laptop	Linux/Windows	4
6	UTA device	USB device	——	4
7	AP node	Openwrt	Embedded Linux	4

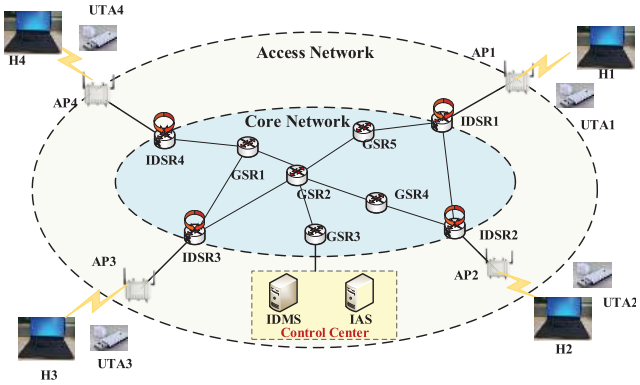


FIGURE 6. The topology of the prototype system.

B. DEPLOYMENT ENVIRONMENT

The MFC prototype system satisfies the requirements of access-core isolation and controllability. Besides, the actual deployment environment is based on the combination of virtual software and physical devices. The platform software is installed on the servers by using the virtualization software VMware ESXi 6.7, and management software of data centers, i.e., vSphere Center Server 6.7 is installed on an Inspur server. The specific equipment deployment and environment are shown in Table 3.

C. VERIFICATION SCENARIOS

The verification scenario mainly involves performance tests of the MFC framework, including the following aspects:

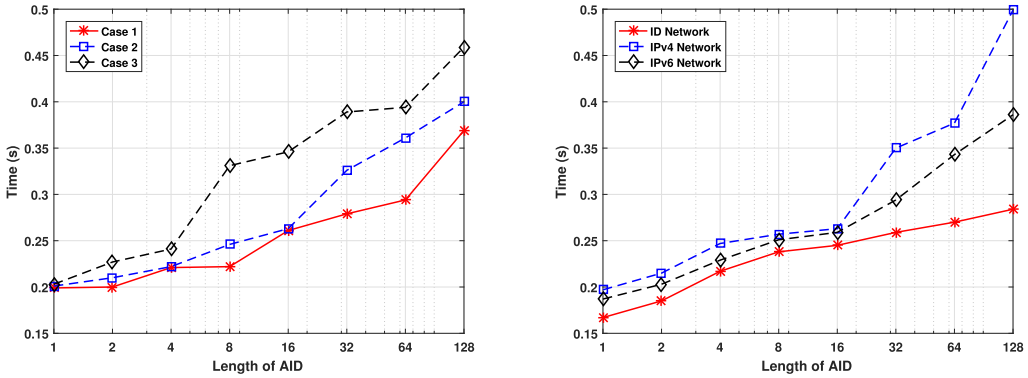
1) Unified access control and management for registered users: This experiment is to verify whether the essential functions of the proposed framework are complete and comprehensive, whether it supports the registration and authentication of legitimate users and shields illegal users from the core network.
2) Support user concurrent access authentication: This experiment is to verify whether the authentication framework can provide regular access services in the case of high user concurrency, so as not to cause the system failure. Besides, we need to verify the impact of different user concurrency on authentication delay.
3) Average delay test of user authentication: This experiment is to confirm that the time complexity of the MFC framework is low enough and to achieve lower latency performance in large user concurrency and mobile authentication. In addition, we verify the system's authentication delay performance under different system parameters.

V. IMPLEMENTATION & EXPERIMENTAL RESULTS

In this section, we test performances of the MFC framework based on the prototype system and verify the impact of various parameters, such as the number of user concurrency, the length of the AID, and the number of registered users on the time cost. We compare different parameter configurations and three network structures, i.e., IPv4, IPv6 and IDentifier Network (i.e., ID Network). We implement the basic authentication process over the IPv4 and IPv6 networks and then compared them with the proposed complete identifier

TABLE 3. The deployment environment of the MFC framework.

Num	Equipments classification	Device/software name	Configuration and deployment	Count
1	Platform software	VMware ESXi6.7	Server virtual software, installed on each server, each server can install multiple virtual machines	——
		vSphere Center Server6.7	Data center host management software that manages all deployed server hosts, deployed on the wave server	——
2	Kernal hardware	Dell EMC Server R740	•Intel Xeon Silver 4210 2.2G, 10C/20T, 9.6GT/s,13.75M •DRAM 2x32GB •SAS 600GB •Intel X710 2x10GbE SFP+ •Intel i350 2x1GbE BASE-T	3
		Dell terminals	•Intel Core i7-6700 3.4G, 4C/8T •DRAM 8GB •SSD 1TB •1x1GbE BASE-T •Ubuntu Linux 14.04 SP1	4
		INSPUR Server	•Xeon E5-2609 v3 1.9GHZ •24x1GBe BASE-T •4x1GbE SFP+	1
		HUAWEI Switch	•S5720-28P-SI-AC •24x1GBe BASE-T •4x1GbE SFP+	1



(a) AID length variations under three configurations.

(b) AID length variations under three networks.

FIGURE 7. The influence of AID length on authentication.

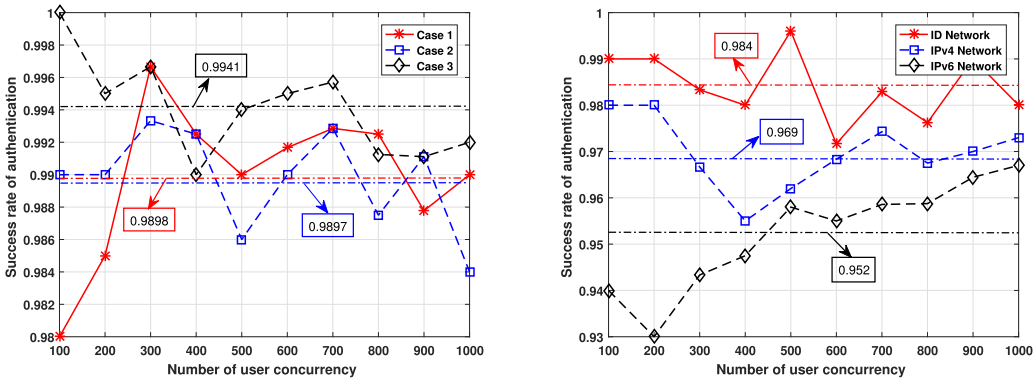
authentication framework including AID and RID information. Finally, we compare various types of security solutions.

During the authentication process, the system involves three necessary system parameter settings: maximum request time, cleanup delay, and the maximum number of requests. The maximum request time specifies the maximum time to process a request packet, the cleanup delay specifies the wait time before a reply returns to the agent data, and the maximum number of requests specifies the maximum number of requests the server can record. In the following comparisons, we set three cases (Case 1: 10, 2, 256. Case 2: 50, 5, 1000. Case 3: 120, 10, 10000) and test the verification time overhead with the change of parameters in three cases.

A. THE IMPACT OF AID LENGTH ON AUTHENTICATION

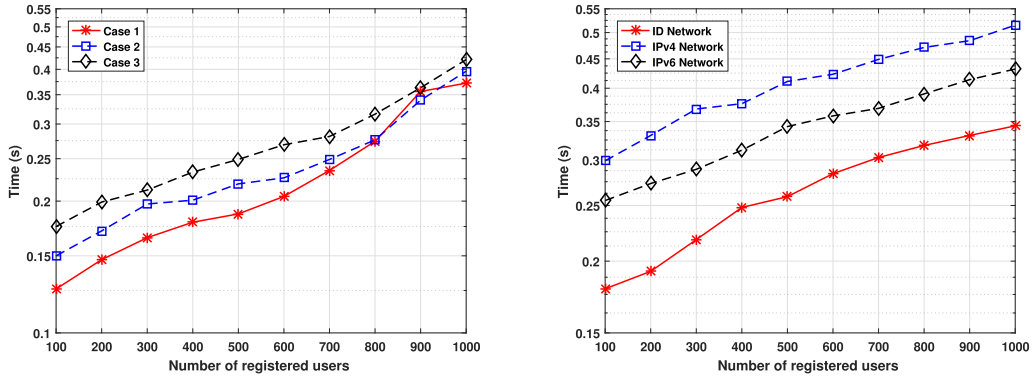
The AID identifies the user's uniqueness and serves as one of the authentication information. Its length affects our time overhead. In Figure 7 (a), we set three cases. The time overhead becomes larger as the length of the AID increases in all three cases. When the length is between 1-4 bytes, the change is slightly relieved, and when the length exceeds 4 bytes, the time loss of Case 3 suddenly increases. When the length exceeds 16 bytes, the growth rate of the other two cases also begins to accelerate. Overall, the time cost of Case 3 is slightly more severe than in the other two cases. When the length reaches 128 bytes, the time cost is close to one-half second. Although a longer AID enhances system security, it increases the time cost.

Based on the parameters of Case 1, Figure 7 (b) illustrates the effect of AID length on different networks. We give the authentication delays under the IPv4, IPv6, and ID networks, respectively. We can see from the figure that the ID network has a lower authentication delay and is optimized by 28.2% and 44% respectively compared with the other two cases. Starting from 16 bytes, the change of authentication delay in the IPv4 and IPv6 networks is growing faster, and the authentication under the ID network is still flat. According to the results, the proposed framework effectively optimizes the time cost.



(a) Concurrency tests under three configurations. (b) Concurrency tests under three networks.

FIGURE 8. The influence of user concurrency on authentication.



(a) Registered user variations under three configurations. (b) Registered user variations under three networks.

FIGURE 9. The influence of registered users on authentication.

B. THE IMPACT OF USER CONCURRENCY ON AUTHENTICATION

The number of user concurrency affects network congestion and tests the processing capacity of IAS, which inevitably leads to the situation where authentication fails. In the context of the background flow, Figure 8 (a) illustrates the authentication success rate for different system configurations. As the number of concurrent users increases, the value of three cases fluctuates but remains above 90 per cent. Before the value of concurrent users reaches 300, the success rate in Case 1 is superior to other cases. When the number of users exceeds 300, the authentication success rate of all three configurations begins to show a downward trend. Also, we calculate the average value of the three cases, i.e., 0.9898, 0.9897, and 0.9941. Overall, Case 2 is slightly better than the other two configurations.

In Figure 8 (b), we compare the authentication success rate of the three networks as the number of user concurrency changes. As the number of simultaneous requests increases, the gap between the three networks narrows, and the ID network with the red line is superior to the other two scenarios. The overall value of them is relatively stable, and the average authentication success rate for three protocol network architectures was 98.4%, 96.9% and 95.2%, respectively. The network using the identifier mapping mechanism is more suitable for security networks.

C. THE IMPACT OF REGISTERED USER NUMBER ON AUTHENTICATION

The number of registered users in IAS affects the speed at which authentication information is searched, which has an essential impact on the authentication efficiency of the system. Figure 9 (a) illustrates the effect of the number of registered users on the authentication delay. When the number is between 100 and 600, the growth rate of the three cases is relatively stable. When the number exceeds 600, the increase rate of the three cases is accelerated. In particular, the time loss of Case 1 is gradually deteriorated, and when the number of users reaches 800, the value exceeds Case 2. Overall, Case 1 is still optimal.

As shown in Figure 9 (b), we give the effects of registered users on three networks. On the whole, the time cost of the three architectures slowly grows, and there is no significant difference. In addition, the time cost of the ID network framework is reduced by 38.4% and 46.7%, respectively, compared to the other two structures.

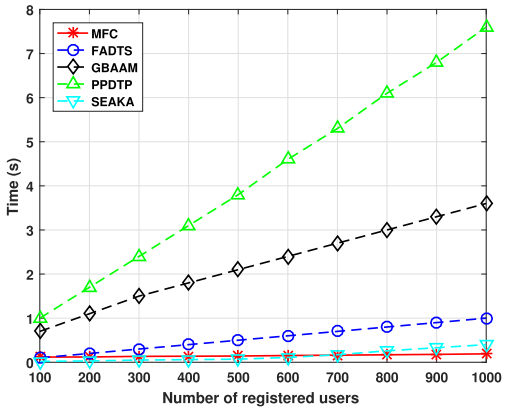


FIGURE 10. Time of various schemes.

D. TIME COMPARISON OF VARIOUS SCHEMES

In addition to the above internal tests, we compared the time cost of different security schemes based on the results of Paper [46]. In Figure 10, we present a comparison of the delays for five security schemes as the number of users increases. From the figure, we can see that the PDDTP scheme has the largest authentication delay, and our proposed scheme delay is similar to the SEAKA scheme. Even before the number of users reached 700, the SEAKA solution was superior to the framework we proposed. Since the increase rate of the proposed scheme is less than that of SEAKA, the proposed scheme is optimal when the number is higher than 700. The final result gives that our proposed scheme is better than 97.3%, 94.4%, 80%, and 33.3% respectively than the other four schemes.

VI. CONCLUSION

Network openness and security are mutually contradictory. As the 5G era has driven the development of relevant technologies, it has also brought potential threats to network security. Especially, massive device access places enormous pressures on the network user side. As we discussed in this paper, it is critical to fleetly detect, eliminate attacks and keep malicious data out of the core network at the edge of networks. Therefore, we proposed the MFC framework, which satisfies the security criteria of 1) network and userspace isolation; 2) user unique identification; 3) biometric feature; 4) hardware access device; 5) user fine-grained attribute control; and 6) bidirectional control. First, we investigated the existing security schemes, including encryption, access control, and security monitoring technologies, then comprehensively discussed respective effects and limitations. Second, the model structure and implementation process of MFC were introduced, which includes the generation of AID identifier and the definition of protocol fields. A novel identifier mapping mechanism from the user side to the core network (i.e., the conversion between AIDs and RIDs) was designed to realize network isolation. To illustrate the functions of MFC, we performed theoretical comparisons among diversified schemes. Third, the MFC prototype system with the wireless deployment environment was established to test the superiority of this framework. The system kernel was modified in depth to support the functions of MFC. Finally, experimental results validated the advantages of MFC, in terms of low latency and high concurrencies.

Attack and defence can be treated as a game process. Nowadays, 5G is facing many unknown security challenges. In the future, we will further optimize the authentication framework to resist unpredictable attacks via adopting the ''service classification''. In the core network, for instance, it is non-privileged for low-level users to access the high-level services. Therefore, the reduction of threats in the core networks is expected.

ACKNOWLEDGMENT

The authors would like to thank all the reviewers and editors for their invaluable comments and efforts on this article.

REFERENCES

[1] *Cyber Attack Trends: 2019 Mid-Year Report*. Accessed: Oct. 14, 2019. [Online]. Available: https://www.checkpoint.com/downloads/resources/cyber-attack-trends-mid-year-report-2019.pdf

[2] *Radware has Released Its 2018-2019 Global Application and Network Security Report*. Accessed: Oct. 14, 2019. [Online]. Available: https://www.radware.com/documents/infographics/trust-factor-cybersecurity-sustaining-business

[3] Z.-Y. Ai, Y.-T. Zhou, and F. Song, "A smart collaborative routing protocol for reliable data diffusion in IoT scenarios," *Sensors*, vol. 18, no. 6, p. 1926, Jun. 2018.

[4] H. Hui, C. Zhou, S. Xu, and F. Lin, "A novel secure data transmission scheme in industrial Internet of Things," *China Commun.*, vol. 17, no. 1, pp. 73–88, 2020.

[5] M. A. Mughal, X. Luo, A. Ullah, S. Ullah, and Z. Mahmood, "A lightweight digital signature based security scheme for human–centered Internet of Things," *IEEE Access*, vol. 6, pp. 31630–31643, 2018.

[6] T.-Y. Wu, C.-M. Chen, K.-H. Wang, and J. M.-T. Wu, "Security analysis and enhancement of a certificateless searchable public key encryption scheme for IIoT environments," *IEEE Access*, vol. 7, pp. 49232–49239, 2019.

[7] M. Ma, D. He, N. Kumar, K.-K.-R. Choo, and J. Chen, "Certificateless searchable public key encryption scheme for industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 14, no. 2, pp. 759–767, Feb. 2018.

[8] U. Khadam, M. M. Iqbal, M. A. Azam, S. Khalid, S. Rho, and N. Chilamkurti, "Digital watermarking technique for text document protection using data mining analysis," *IEEE Access*, vol. 7, pp. 64955–64965, 2019.

[9] Q. Li, R. Sandhu, X. Zhang, and M. Xu, "Mandatory content access control for privacy protection in information centric networks," *IEEE Trans. Dependable Secure Comput.*, vol. 14, no. 5, pp. 494–506, Sep. 2017.

[10] M. Ghafoorian, D. Abbasinezhad-Mood, and H. Shakeri, "A thorough trust and reputation based RBAC model for secure data storage in the cloud," *IEEE Trans. Parallel Distrib. Syst.*, vol. 30, no. 4, pp. 778–788, Apr. 2019.

[11] J. P. Cruz, Y. Kaji, and N. Yanai, "RBAC-SC: Role-based access control using smart contract," *IEEE Access*, vol. 6, pp. 12240–12251, 2018.

[12] S. Jha, S. Sural, V. Atluri, and J. Vaidya, "Security analysis of ABAC under an administrative model," *IET Inf. Secur.*, vol. 13, no. 2, pp. 96–103, Mar. 2019.

[13] W. Bul'ajoul, A. James, and S. Shaikh, "A new architecture for network intrusion detection and prevention," *IEEE Access*, vol. 7, pp. 18558–18573, 2019.

[14] J. Jingping, C. Kehua, C. Jia, Z. Dengwen, and M. Wei, "Detection and recognition of atomic evasions against network intrusion detection/prevention systems," *IEEE Access*, vol. 7, pp. 87816–87826, 2019.

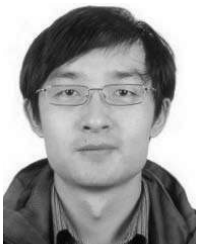
[15] K. Cao and A. K. Jain, "Automated latent fingerprint recognition," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 41, no. 4, pp. 788–800, Apr. 2019.

[16] W. Fan, Z. Du, M. Smith-Creasey, and D. Fernandez, "HoneyDOC: An efficient honeypot architecture enabling all–round design," *IEEE J. Sel. Areas Commun.*, vol. 37, no. 3, pp. 683–697, Mar. 2019.
[17] F. Song, Y.-T. Zhou, L. Chang, and H.-K. Zhang, "Modeling space–terrestrial integrated networks with smart collaborative theory," *IEEE Netw.*, vol. 33, no. 1, pp. 51–57, Jan. 2019.
[18] Z. Ai, Y. Liu, F. Song, and H. Zhang, "A smart collaborative charging algorithm for mobile power distribution in 5G networks," *IEEE Access*, vol. 6, pp. 28668–28679, 2018.
[19] H. Yin, J. Zhang, Y. Xiong, L. Ou, F. Li, S. Liao, and K. Li, "CP–ABSE: A ciphertext–policy attribute–based searchable encryption scheme," *IEEE Access*, vol. 7, pp. 5682–5694, 2019.
[20] Z. Liu, J. Xu, Y. Liu, and B. Wang, "Updatable ciphertext–policy attribute–based encryption scheme with traceability and revocability," *IEEE Access*, vol. 7, pp. 66832–66844, 2019.
[21] W. Huang, Y. Liao, S. Zhou, and H. Chen, "An efficient deniable authenticated encryption scheme for privacy protection," *IEEE Access*, vol. 7, pp. 43453–43461, 2019.
[22] Y. Chen, Y. Ge, Y. Wang, and Z. Zeng, "An improved three–factor user authentication and key agreement scheme for wireless medical sensor networks," *IEEE Access*, vol. 7, pp. 85440–85451, 2019.
[23] A. Sengupta, E. R. Kumar, and N. P. Chandra, "Embedding digital signature using encrypted–hashing for protection of DSP cores in CE," *IEEE Trans. Consum. Electron.*, vol. 65, no. 3, pp. 398–407, Aug. 2019.
[24] J. Chen, M. Tian, C. Gao, and Z. Chen, "A lattice–based incremental signature scheme," *IEEE Access*, vol. 7, pp. 21201–21210, 2019.
[25] Y. Xie, H. Wen, B. Wu, Y. Jiang, and J. Meng, "A modified hierarchical attribute–based encryption access control method for mobile cloud computing," *IEEE Trans. Cloud Comput.*, vol. 7, no. 2, pp. 383–391, Apr. 2019.
[26] G. Fedrecheski, L. C. C. De Biase, P. C. Calcina-Ccori, and M. K. Zuffo, "Attribute–based access control for the swarm with distributed policy management," *IEEE Trans. Consum. Electron.*, vol. 65, no. 1, pp. 90–98, Feb. 2019.
[27] S. Ding, J. Cao, C. Li, K. Fan, and H. Li, "A novel attribute–based access control scheme using blockchain for IoT," *IEEE Access*, vol. 7, pp. 38431–38441, 2019.
[28] Y. Xue, K. Xue, N. Gai, J. Hong, D. S. L. Wei, and P. Hong, "An attribute–based controlled collaborative access control scheme for public cloud storage," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 11, pp. 2927–2942, Nov. 2019.
[29] D. Li, J. Liu, Q. Wu, and Z. Guan, "Efficient CCA2 secure flexible and publicly–verifiable fine–grained access control in fog computing," *IEEE Access*, vol. 7, pp. 11688–11697, 2019.
[30] Y.-H. Lin, J.-J. Huang, C.-I. Fan, and W.-T. Chen, "Local authentication and access control scheme in M2M communications with computation offloading," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 3209–3219, Aug. 2018.
[31] K. Xue, P. He, X. Zhang, Q. Xia, D. S. L. Wei, H. Yue, and F. Wu, "A secure, efficient, and accountable edge–based access control framework for information centric networks," *IEEE/ACM Trans. Netw.*, vol. 27, no. 3, pp. 1220–1233, Jun. 2019.
[32] W. Xiong, F. Zhou, R. Wang, R. Lan, X. Sun, and X. Luo, "An efficient and secure two–factor password authentication scheme with card reader (terminal) verification," *IEEE Access*, vol. 6, pp. 70707–70719, 2018.
[33] S. Garg, K. Kaur, N. Kumar, and J. J. P. C. Rodrigues, "Hybrid deep-learning-based anomaly detection scheme for suspicious flow detection in SDN: A social multimedia perspective," *IEEE Trans. Multimedia*, vol. 21, no. 3, pp. 566–578, Mar. 2019.
[34] L. F. Maimo, A. L. P. Gomez, F. J. G. Clemente, M. G. Perez, and G. M. Perez, "A self–adaptive deep learning–based system for anomaly detection in 5G networks," *IEEE Access*, vol. 6, pp. 7700–7712, 2018.
[35] M. A. Reshan, H. Liu, C. Hu, and J. Yu, "MBPSKA: Multi–biometric and physiological signal–based key agreement for body area networks," *IEEE Access*, vol. 7, pp. 78484–78502, 2019.
[36] V. Sharma, R. Kumar, W.-H. Cheng, M. Atiquzzaman, K. Srinivasan, and A. Zomaya, "NHAD: Neuro–fuzzy based horizontal anomaly detection in online social networks," *IEEE Trans. Knowl. Data Eng.*, vol. 30, no. 11, pp. 2171–2184, Nov. 2018.
[37] Y. Meng, T. Qin, Y. Liu, and C. He, "An effective high threating alarm mining method for cloud security management," *IEEE Access*, vol. 6, pp. 22634–22644, 2018.
[38] L. Shi, Y. Li, T. Liu, J. Liu, B. Shan, and H. Chen, "Dynamic distributed honeypot based on blockchain," *IEEE Access*, vol. 7, pp. 72234–72246, 2019.
[39] F. Song, Y.-T. Zhou, Y. Wang, T.-M. Zhao, I. You, and H.-K. Zhang, "Smart collaborative distribution for privacy enhancement in moving target defense," *Inf. Sci.*, vol. 479, pp. 593–606, Apr. 2019.
[40] D. Wang and P. Wang, "Two birds with one stone: Two–factor authentication with security beyond conventional bound," *IEEE Trans. Dependable Secure Comput.*, vol. 15, no. 4, pp. 708–722, Jul./Aug. 2018.
[41] T. Maitra, M. S. Obaidat, S. H. Islam, D. Giri, and R. Amin, "Security analysis and design of an efficient ECC-based two-factor password authentication scheme," *Secur. Commun. Netw.*, vol. 9, no. 17, pp. 4166–4181, Nov. 2016.
[42] Q. Xie, N. Dong, D. S. Wong, and B. Hu, "Cryptanalysis and security enhancement of a robust two-factor authentication and key agreement protocol," *Int. J. Commun. Syst.*, vol. 29, no. 3, pp. 478–487, Feb. 2016.
[43] X. Li, J. Niu, S. Kumari, J. Liao, W. Liang, and M. K. Khan, "A new authentication protocol for healthcare applications using wireless medical sensor networks with user anonymity," *Secur. Commun. Netw.*, vol. 9, no. 15, pp. 2643–2655, Oct. 2016.
[44] Y. Park, S. Lee, C. Kim, and Y. Park, "Secure biometric-based authentication scheme with smart card revocation/reissue for wireless sensor networks," *Int. J. Distrib. Sensor Netw.*, vol. 12, no. 7, Jul. 2016, Art. no. 155014771665860.
[45] F. Song, Z. Ai, Y. Zhou, I. You, K.-K. R. Choo, and H. Zhang, "Smart collaborative automation for receive buffer control in multipath industrial networks," *IEEE Trans. Ind. Informat.* To be published.
[46] J. Cao, P. Yu, M. Ma, and W. Gao, "Fast authentication and data transfer scheme for massive NB–IoT devices in 3GPP 5G network," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1561–1575, Apr. 2019.

ZHENGYANG AI received the B.S. degree from the School of Computer and Information Technology, Northeast Petroleum University, in 2016. He is currently pursuing the Ph.D. degree with the National Engineering Laboratory for Next-Generation Internet Technology, School of Electronics and Information Engineering, Beijing Jiaotong University. His current research interests include network architecture and network security.

YING LIU received the M.S. and Ph.D. degrees from Beijing Jiaotong University, Beijing, China, in 2003 and 2012, respectively. Since 2012, she has been an Associate Professor with the National Engineering Laboratory for Next-Generation Internet Technology, School of Electronic and Information Engineering, Beijing Jiaotong University. Her current research interests include network architecture, network security, protocol optimization, wireless communications, and cloud computing.

LIU CHANG is currently with the Network Technology Research Institute, China Unicom. He has published many academic articles in well-known international journals. His current research interests include network modeling, IP and bearer technology, differentiated services, and user experience.



FUHONG LIN received the M.S. and Ph.D. degrees in electronics engineering from Beijing Jiaotong University, Beijing, China, in 2006 and 2010, respectively. He is currently an Associate Professor with the Department of Computer and Communication Engineering, University of Science and Technology Beijing, China. His research interests include edge/fog computing, network security, and big data. He received the Provincial and Ministry Science and Technology Progress Award 2, in 2017. He also received the track Best Paper Award from IEEE/ACM ICCAD, in 2017. His two articles won Top 100 most Cited Chinese Papers Published in International Journals, in 2015 and 2016. He has served as the Co-Chair for the first and third IET International Conference on Cyberspace Technology and the General Chair for the second IET International Conference on Cyberspace Technology. He also serves as a Reviewer for more than ten international journals, including the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE ACCESS, *Information Sciences*, the IEEE INTERNET OF THINGS JOURNAL, *The Computer Journal*, and *China Communications*. He was the leading Editor of the Special issue Recent Advances in Cloud-Aware Mobile Fog Computing for Wireless Communications and Mobile Computing.

FEI SONG is currently a Full Professor with the National Engineering Laboratory for Next Generation Internet Technology, School of Electronic and Information Engineering, Beijing Jiaotong University. He is also with the China University of Petroleum-Beijing at Karamay. His current research interests include network architecture, system security, protocol optimization, and cloud computing. He serves as a Technical Reviewer for several journals, including the *IEEE Communications Magazine*, the IEEE INTERNET OF THINGS JOURNAL, the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, the IEEE TRANSACTIONS ON SERVICES COMPUTING, and the IEEE TRANSACTIONS ON EMERGING TOPICS IN COMPUTING.