A Security Awareness and Protection System for 5G Smart Healthcare Based on Zero-Trust Architecture

Baozhan Chen, Siyuan Qiao, Jie Zhao, Dongqing Liu, Xiaobing Shi, Minzhao Lyu, Haotian Chen, Huimin Lu, *Senior Member, IEEE*, and Yunkai Zhai

***Abstract*—The key features of 5G network (i.e., high bandwidth, low latency, and high concurrency) along with the capability of supporting big data platforms with high mobility make it valuable in coping with emerging medical needs, such as COVID-19 and future healthcare challenges. However, enforcing the security aspect of a 5G-based smart healthcare system that hosts critical data and services is becoming more urgent and critical. Passive security mechanisms (e.g., data encryption and isolation) used in legacy medical platforms cannot provide sufficient protection for a healthcare system that is deployed in a distributed manner and fail to meet the need for data/service sharing across "cloud-edge-terminal" in the 5G era. In this article, we propose a security awareness and protection system that leverages zero-trust architecture for a 5G-based smart medical platform. Driven by the four key dimensions of 5G smart healthcare including "subject" (i.e., users, terminals, and applications), "object" (i.e., data, platforms, and services), "behavior," and "environment," our system constructs trustable dynamic access control models and achieves real-time network security situational awareness, continuous identity authentication, analysis of access behavior, and fine-grained access control. The proposed security system is implemented and tested thoroughly at industrial-grade, which proves that it satisfies the needs of active defense and end-to-end security enforcement of data, users, and services involved in a 5G-based smart medical system.**

Manuscript received August 20, 2020; revised October 23, 2020; accepted November 24, 2020. Date of publication November 30, 2020; date of current version June 23, 2021. This work was supported in part by the National Key Research and Development Program of China under Grant 2017YFC0909900; in part by the National Natural Science Foundation of China under Grant 71673254; in part by the Innovation Research Team of Higher Education in Henan Province under Grant 20IRTSTHN028; and in part by the Zhengzhou Municipal Science and Technology Major Project under Grant 2020YJGG0003. *(Corresponding author: Yunkai Zhai.)*

Baozhan Chen, Jie Zhao, Dongqing Liu, Xiaobing Shi, and Haotian Chen are with the National Engineering Laboratory for Internet Medical Systems and Application and the National Telemedicine Center of China, First Affiliated Hospital of Zhengzhou University, Zhengzhou 450052, China (e-mail: cbz-3-3@163.com; zhaojie@zzu.edu.cn; liudongqing@outlook.com; shixiaobingsdu@foxmail.com; chenhtian@sina.com).

Siyuan Qiao is with the Strategic Investment and Ecological Cooperation Department, Qi An Xin Technology Group Inc., Beijing 100032, China (e-mail: qiaosiyuan@qianxin.com).

Yunkai Zhai is with the National Engineering Laboratory for Internet Medical Systems and Applications and the National Telemedicine Center of China, First Affiliated Hospital of Zhengzhou University, Zhengzhou 450052, China, and also with the Management Engineering School, Zhengzhou University, Zhengzhou 450000, China (e-mail: zhaiyunkai@zzu.edu.cn).

Minzhao Lyu is with the School of Electrical Engineering and Telecommunications, University of New South Wales, Sydney, NSW 2052, Australia, and also with Data61, CSIRO, Sydney, NSW 2015, Australia (e-mail: minzhao.lyu@unsw.edu.au).

Huimin Lu is with the Department of Mechanical and Control Engineering, Kyushu Institute of Technology, Kitakyushu 804-8550, Japan (e-mail: dr.huimin.lu@ieee.org).

Digital Object Identifier 10.1109/JIOT.2020.3041042

***Index Terms*—5G, security and privacy, smart healthcare, zero-trust architecture (ZTA).**

I. Introduction

With the development and wide adoption of 5G technology, a series of changes introduced by "Internet+" and "Smart+" facilitate the "intellectualization" of the society, and this trend is also reflected in the healthcare industry [7]. 5G technology is characterized by new air interface, service-oriented network architecture, and end-to-end network slicing [17], [19], [22], which can adapt to the network requirements of different applications. Furthermore, 5G provides powerful technical support for developments of smart medical applications and 5G healthcare is one of the most important application areas of 5G technology in vertical industries. 5G presents a strong vitality in the medical industry, it has the abilities in supporting massive medical image data transferring and processing, ultrahigh-definition video interaction, and real-time remote control of smart devices [6], [30], thus can satisfy the network needs of multidisciplinary consultation, intelligent diagnosis of medical images, remote surgery, and other medical application scenarios [9], [20]. However, the medical industry is involved in the problems of centralized medical resources, high-dense personnel, sophisticated information systems, and a large variety of heterogeneous medical equipment. Since many medical application scenarios need to integrate different medical equipment, applications, and services, 5G faces lots of challenges when applied to the medical industry.

5G smart healthcare is one of the future directions of the healthcare service model, it integrates different technologies, i.e., 5G, Internet of Things (IoT), edge computing, fog computing, and artificial intelligence [13]. Based on the concepts of mobile healthcare, telemedicine, and Internet healthcare, innovations happen on 5G smart healthcare, such as new healthcare service models and products. In July 2020, 3rd Generation Partnership Project (3GPP) announced the official complement of the R16 version of 5G, which indicates that the technical solution of 5G smart healthcare will be further clarified. All kinds of 5G smart healthcare production are expected to be accelerated and many of them will be more accessible to the public once the standardization and security requirements are reached. According to IHS Markit, the health and fitness market empowered by 5G will be more than one trillion dollars.

5G accelerates the upgrade of the medical industry and gains great attention from all over the world. Many countries have stepped into the application and development of 5G smart healthcare and have carried out a series of research and innovative practices in 5G healthcare network constructions and applications [10]. For example, Verizon officially announced that it would deploy a 5G commercial wireless network and 5G core network in America in the second half of 2018. In October 2018, China Mobile, and the First Affiliated Hospital of Zhengzhou University demonstrated that under the 5G network, doctors could perform remote ultrasound operations and real-time diagnosis. Vodafone and Clínic Hospital collaborated on 5G-based remote surgery experiments in February 2019, with the aim to build the first 5G smart hospital in Spain. In June 2019, the University Hospital of Birmingham, U.K., in partnership with British Telecom and west midlands 5G (WM5G), demonstrated the possibility of 5G ambulance and remote ultrasound operations. In October 2019, Huawei, China Mobile and The first Affiliated Hospital of Zhengzhou University published a white paper related to a 5G medical network based on elastic network slicing. In April 2020, Sichuan University and China Mobile released a COVID-19 immune detection and analysis system based on 5G cloud computing, where 5G remote CT system was used in the prevention and control of COVID-19.

However, 5G smart healthcare faces critical security and privacy issues [15] than legacy healthcare services. 5G medical applications change traditional medical services by extending them from hospital to online service mode which involved with many users, medical devices, information systems, and is accompanied by massive medical data transmission, thus, serious security and privacy challenges are introduced with 5G medical applications. Security vulnerabilities in terminals, networks, and systems will seriously affect the quality of medical services and the normal operations of medical institutions [2]. Meanwhile, 5G security standards and 5G medical industry security standards have not yet been established, and it is still unclear on how to implement security protection and risk management for 5G medical applications.

Zero-trust architecture (ZTA) that was proposed in [12] appears to be a proper solution for 5G security as it holds the assumption that by default, any person, event, or device inside and outside a network and information system is untrustworthy before sufficient verification and authentication. The ideology of "zero-trust" meets the security requirements of a 5G network that hosts a massive number of connected devices and sessions with uncertain risks. However, existing "zero-trust" frameworks mainly consider subjects (e.g., clients and servers) and objects (e.g., requested data) during a network session, which do not fully cover all potential security risks introduced by changing environments and behaviors of mobile entities under 5G smart healthcare scenarios.

To this end, we propose a security awareness and protection system leveraging ZTA for 5G-based smart healthcare. In this article, we have achieved four specific contributions.

1) We highlighted security threats faced by smart healthcare and 5G network, and articulated requirements for security and privacy of 5G smart healthcare systems. We then note that zero-trust concept that assumes all entities involved are not trustable unless authorized or confirmed to be secure is a viable solution, however, it needs to be extended for scenarios of 5G smart healthcare.
2) We come up with a four-dimensional security framework using ZTA [23] for 5G smart medical systems. The four core dimensions (i.e., subject, object, environment, and behavior) of access are collectively used by risk judgment mechanism, trust assessment model, and access control model to continuously assess potential risks at all aspects and perform fine-grained session-based access control.
3) Based on the concept of our four-dimensional security framework, we proposed our design of a security awareness and protection system for 5G smart healthcare, with emphasis on the security enforcements for virtualized networks, IoT accesses, medical data collaborations, and integrated 5G network security.
4) We implemented and tested our proposed system thoroughly for its functionality and system performance during industrial grade operations. Testing results demonstrate that our system is an effective and high-quality security solution for 5G smart medical applications.

The remainder of this article is organized as follows. Section II describes security risks and requirements of 5G smart healthcare; Section III introduces our zero-trust four-dimensional security framework and its key components; Section IV discusses the design and its key principles of our security awareness and protection system leveraging the proposed zero-trust four-dimensional framework for 5G smart healthcare. Section V illustrates evaluation results of our implemented system under a production-level testing environment; And this article is concluded in Section VI.

II. Security Requirements of 5G Smart Healthcare

A variety of medical application scenarios has appeared or been improved with 5G smart healthcare. For example, remote consultation, remote surgery, remote teaching, remote emergency rescue, and remote monitoring have been rapidly developed based on 5G technology [21], [26], [30]. While improving the quality of hospital services and enhancing the patient experience, these application scenarios bring new security challenges. Since medical information contains a lot of privacy of users and some medical application scenarios impact the safety of patients, the security aspect of 5G medical healthcare will play significant roles in national, network, and information security [3], [24].

A. Security Threats Faced by Smart Healthcare

Security threats faced by smart healthcare services [5], [11], [18], [27], [31] can be briefly categorized into the following aspects.

1) *Large-Scale Monitoring and Theft of Medical Data and Patient Privacy Information:* 5G medical applications involve privacy information, such as electronic medical records, medical images, and medical laboratory data.

The leakage of such information which may be analyzed by powerful big data technologies will seriously threaten the security of medical data and the protection of patient privacy.

2) *Attacks on Critical Infrastructures of 5G Healthcare Network:* Many application scenarios, i.e., remote surgery and emergency rescue, have critical requirements on the reliability and transmission delay of 5G network. If the network infrastructure of such applications is attacked and paralyzed, it will cause serious impacts on the lives of patients.
3) *Malicious Data Tampering of Medical Records:* The capabilities of 5G enable the collection of wide-scale, large-scale medical, and health data. The collected data can detect and report public health events, such as outbreaks of epidemics and unknown diseases in a timely manner. However, malicious manipulation of collected data will distort the medical records, resulting in failure of surveillance and emergency response mechanisms, which may lead to outbreaks of large-scale public health events.

It is worth noting that the source of above security threats may not only come from external networks but also internal networks.

B. Security Issues of 5G Network

In addition to the above-mentioned security threats to medical applications, 5G smart healthcare also needs to deal with the security issues brought by 5G technology itself [1], [15], [34]. Security risks of 5G network mainly include.

1) The large-scale connectivity of 5G network may incur signaling storms or distributed denial of service (DDoS) attacks. 5G supports 1 million connections/km, and hackers can launch traffic attacks by using massive terminals at the same time, which may destroy network defense capability.
2) The high-bandwidth and low-latency characteristics may increase the difficulty of traffic security protection, content identification, encryption, and decryption. 5G ultra-high bandwidth and low transmission latency requirements put forward strong needs for network security situational awareness, malicious traffic attack prevention, malware monitoring, and other capabilities, as well as the ability to encrypt and decrypt transmitted data, which increases the difficulty of security protection [8], [28].
3) The introduction of edge cloud and Device-to-Device (D2D) communication makes the existing centralized monitoring system ineffective. Edge cloud and D2D communication have changed the original network architecture and communication modes, resulting in more content security risks than centralized management [32]. Moreover, it is more difficult to ensure the traffic security of edge cloud service and D2D communication, since their traffic bypass existing centralized security monitoring systems.

C. Security Requirements of 5G Smart Healthcare

With the security problems of 5G network and the vulnerability of smart healthcare, sufficient and proper security protection for 5G smart medical systems is highly required. The requirements are described as follows.

1) Unified control, intelligent defense, flexible, and scalable 5G smart healthcare system are needed. The security system should satisfy the security requirements of multiple access methods and different medical application scenarios, provide security protection mechanisms for different scenarios with different requirements of bandwidth, latency, and connections.
2) Unified and scalable identification and authentication management mechanisms are needed. The system should meet the security requirements of various types of connected terminals, such as the IoT, and realizes unified management, identification, and traceability of user identity.
3) Distributed security defense capability is needed. Based on the computing power of the central system and the edge system, the system should have distributed security defense capabilities to deal with security threats caused by multiaccess edge computing (MEC) and D2D connections, with the aim to establish an integrated security system that can meet the security protection requirements of 5G smart healthcare.

D. Opportunities by the Zero-Trust Architecture

The above challenges can be handled with the help of ZTA [16]. The ZTA assumes that all network traffic cannot be trusted unless it is authorized, detected, or confirmed to be secure [4]. It ensures secured access to healthcare data, regardless of whether the access location is from an internal or external network.

In the book "Zero Trust Network: Building a Security System in an Untrusted Network" [12], the authors outlined key assumptions for zero-trust security. The network is always in a dangerous environment, and there are external or internal threats throughout the network. Physical location is not enough to determine the credibility of a network. All devices, users, and network traffic should be authenticated and authorized. And security policies must be dynamic and calculated from as many data sources as possible. In short, the zero-trust security framework mainly includes the following ideas.

1) Using identity as the basis of access control.
2) Using "least privilege" principle for resource allocation.
3) Real-time calculation of access control strategy.
4) Only allowing controlled and secured access to resources.
5) Continuous evaluation of trust level from multiple data sources.

The ZTA reduces malicious access and attacks by employing least privilege policies and strictly enforcing access control policies [14], [29], [33]. It detects and logs all network traffic and continuously tracks user behavior. Therefore, the zero-trust model is suitable for addressing the network risks and medical application security challenges faced by 5G smart

healthcare. However, existing zero-trust security frameworks are usually established using the subject (i.e., people, equipment) and the object (i.e., data, services) as core security dimensions [25], [35], which cannot satisfy the security needs of 5G smart medical applications in tracking and defending against risks introduced by distributed environments and changing behaviors.

III. Four-Dimensional Security Framework for 5G Smart Healthcare Based on Zero-Trust Architecture

5G-based Smart healthcare needs to achieve collaborations among terminals, edge computing nodes, and cloud data sharing utilities and applications in a high-bandwidth, low-latency, and high-concurrency environment. Existing security systems using network isolation and defense-in-depth cannot meet emerging defense requirements of 5G smart healthcare as discussed before. Thus, it is necessary to break the physical network boundary and establish a new network security framework based on services and applications to achieve fine-grained security awareness and protection capabilities. As mentioned in Section II-D, current zero-trust security architecture holds promises in satisfying security requirements of 5G smart healthcare while its considered dimensions are not sufficient.

Thus, by expanding the zero-trust concept leveraging only two dimensions, we propose a four-dimensional security framework using the ZTA that focuses on subject (i.e., people, equipment, applications), object (i.e., data, platform, service), environment, and behavior of a 5G smart medical system (Section III). Our framework employs a trusted dynamic access control model (Section III-D) that deciding run-time privileges to achieve real-time situational security awareness, continuous identity authentication, behavior monitoring and analysis, and fine-grained control of access behavior. Access controls are made according to security and trust levels from multiple sources, such as the trust assessment model (Section III-C), while the trust assessment process performs continuous evaluation from four dimensions as well as inference reports from the risk judgment mechanism (Section III-B).

A. Four Security Dimensions of Our Zero-Trust Framework

Now we describe the proposed four dimensions of our zero-trust framework for 5G smart healthcare scenarios.

1) Dimension 1—Subject: First, we define the subject of a 5G smart medical information system. The subject is the party that initiates network and resource access requests. As shown in Fig. 1(a), in a 5G smart healthcare system, the subjects include identity-based medical practitioners, identification-based networked medical and network equipment, and online medical applications bounded with personal identity or device identification. Different subjects may have different trustability, therefore, more trustable subjects (e.g., chief doctors) have the power to access more sensitive resources (e.g., medical records) whereas less trustable subjects (e.g., network-connected smart sphygmomanometers) may have no access to any information but only upload measured data.

Thus, trust level of subjects is the first dimension of 5G smart medical security. A subject's trust level is calculated using real-time data from multiple sources, such as identities, privileges, access logs, and other information. A trust level would have higher accuracy if it is calculated from more types of data with higher reliability. The rapid development of artificial intelligence technologies empowers trust assessment. Artificial intelligence technologies, such as expert systems and machine learning that are closely linked to application scenarios can be used to improve the calculation efficiency of trust assessment strategies and realize the ZTA with security, reliability, availability, and cost-effectiveness.

2) Dimension 2—Object: We now define the object of a 5G smart medical information system, that is, the resource that an access requests. As shown in Fig. 1(b), in a 5G smart healthcare system, objects include medical data, smart medical service functions, and service interfaces. In a smart healthcare scenario, objects are uploaded, downloaded, exchanged, and utilized by subjected. However, operations on objects cannot be unrestricted. As explained before, to guarantee the system security and patient privacy during medical services, sensitive data, service functions, and interfaces should not be accessible to less trustable or irrelevant subjects.

Therefore, security level of objects is the second dimension of 5G smart medical security. An object's security level is calculated from the assessment of its own value, environment, real-time threats, and other information. A security level would have higher accuracy if calculated from more types of data with higher reliabilities.

3) Dimension 3—Environment: We now define the environment of a 5G smart medical information system, that is, the situational security during network and resource access requests and processes. As shown in Fig. 1(c), in a 5G smart medical information system, the environment includes physical, computing, and network environment where medical and network equipment accesses. Although this dimension is usually ignored by existing zero-trust frameworks, it is important as different environments can significantly change the trustability of an access request. For example, accessing sensitive medical records within a private treatment area incurs less privacy risk than accessing them from a shared public region, and providing healthcare services via a private medical network is more secure than the public Internet.

Driven by the above considerations, security level of the access environment is the third dimension of 5G smart medical security. The security level of the environment is calculated from risk awareness (environments of equipment, operation, network, application, and terminal protection, etc.) and threat analysis (risk analysis, trust rating, business linkage, etc.).

4) Dimension 4—Behavior: Finally, the behavior dimension in a 5G smart medical information system is defined. It includes real-time security analysis and judgment based on historical access behavior, current networking behavior, and resource access behavior. In a 5G smart healthcare system [Fig. 1(d)], behavior analysis includes intelligent inference, behavior baseline, security audit, etc. Tracking dynamic and

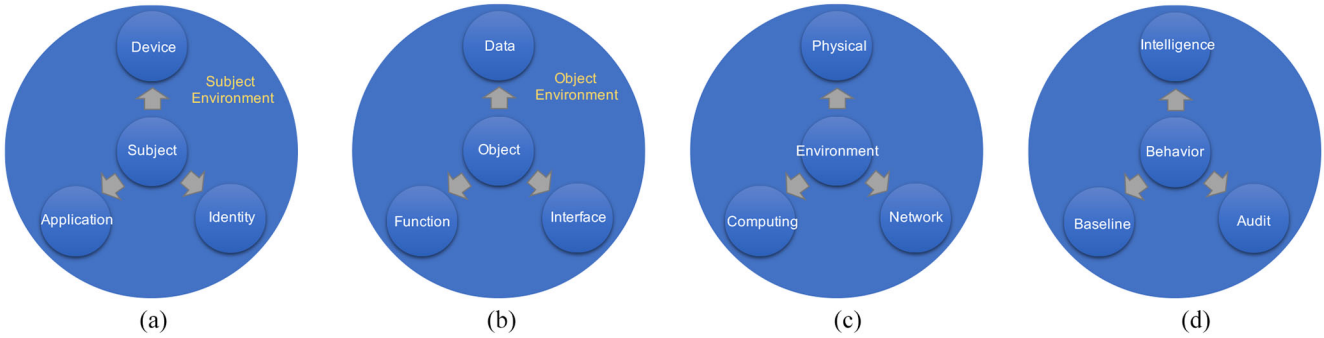

Fig. 1. Four dimensions of 5G smart healthcare security. (a) First dimension—subject. (b) Second dimension—object. (c) Third dimension—environment. (d) Fourth dimension—behavior.

changing behaviors of involved subjects, objects, and environments is of utmost vital in guaranteeing their trustworthiness throughout a service session, as a trustable entity may become untrustable and a secured environment may turn into insecure. Such real-time changes may significantly affect the security and privacy of the delivery of a smart medical service.

Hence, real-time analysis of access behavior is the fourth dimension of 5G smart medical security. Security level of the access behavior is obtained from inputs of external intelligence, audits of historical access behavior, and security monitoring of current access behavior.

B. Risk Judgment Mechanism

Our framework performs risk judgment centered on the dimensions of subject and environment. With subject trust identification and situational awareness, the risk judgment mechanism generates scores and detailed reports on potential risks associated with subjects and environments, which become critical references in the trust assessment process (will be described in Section III-C).

1) Subject- and Environment-Oriented Judgment Mechanism: The risk judgment mechanism of access behavior focuses on the access subject and environment of smart medical applications. The judgment of the subject focuses on "controllability."

1) Whether the identification of networked medical equipment is completed; whether it is registered; and whether it is guaranteed by trusted hardware.
2) Whether the identity of the networked medical personnel is bounded to the device; whether the authentication comes from remote or local sources; what is the method and strength of identity authentication; and what is the personnel information obtained from other systems.
3) Whether the smart medical application has identification; what is the verification status; is there any interference during operation; what is protection strength of application data; and is it started remotely or locally.

In addition, the judgment of the subject needs to consider historical information to make dynamic controllability adjustments.

The judgment of the environment focuses on the "risk level" derived from threat modeling.

1) *Software Environment of Smart Medical Application:* Whether the operating system is safe during startup; what is the level of satisfaction of operating system baseline; what is the patch status; and is there a history of malware attacks, etc.
2) *Computing and Storage Hardware Environment:* What is the temperature of core devices and whether there are additional peripherals.
3) *5G Network Environment:* What is the access location, link type, and capability.
4) *Physical Environments of Connected Medical Equipment:* What is the geographical location and whether it is in a safe enclosed space (e.g., a secured ambulance).
5) *Temporal Environment:* Is it special period (e.g., public holiday) or working hours.

2) Subject Trust Identity: In the 5G smart medical system, identification of medical and network equipment is the most important technology of the subject trust identification. As one of the key technologies in the zero-trust system, the subject trust identification technology needs to be able to uniquely and continuously identify a terminal device. Therefore, the following requirements have to be satisfied.

1) *Available:* Identification should always be able to be calculated regardless of attacks or users' misbehaviors; and he situation that identification cannot be calculated should be treated as exceptions.
2) *Trustworthy:* Identification cannot be counterfeited either by people who have full authorities of the terminal or by attackers (e.g., sniffers).
3) *Unchanged:* Identification needs to be protected from being destroyed; destroyed identification should be able to be detected and restored. An identification should not be changed when the device's core hardware and operating system have not changed; and identification should remain unchanged for the same set of hardware even under virtual environments, such as cloud desktops.
4) *Unique:* Different devices are expected to have unique identifications; and the identification of a device should be changed if the core hardware of the same system (e.g., hard disk) is changed or the operating system is reinstalled.
5) *Stable:* Even if the device has temporary failures, such as damages on disks or there are additions of new

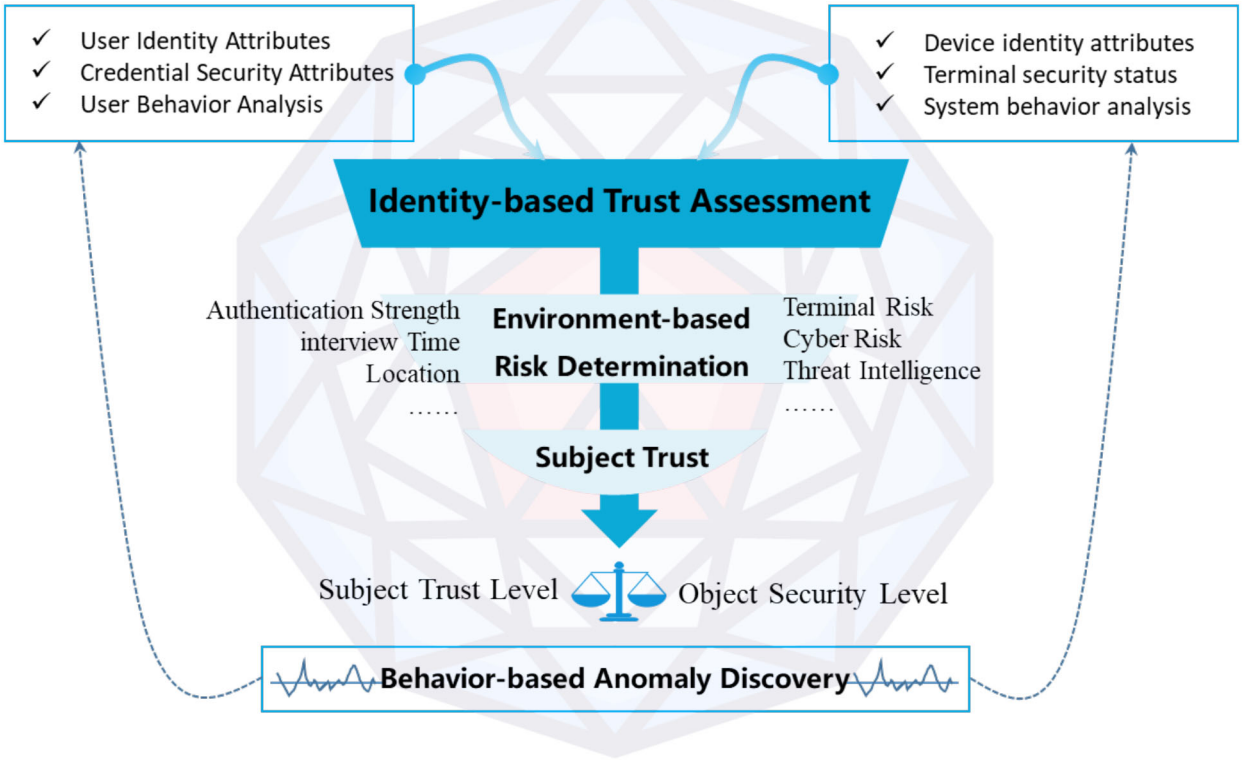

Fig. 2. Our trust assessment model.

peripherals, identification of this device should not be changed immediately; and the identification should not be changed frequently due to its own bug.

3) Situational Awareness: The situational awareness system can simultaneously perceive the trustworthiness of physical, network, and computing environment in a 5G smart medical system through monitoring a variety of clients and dedicated devices. The system uses security policies to determine access behaviors of different trust levels. As a completed zero-trust system, the situational awareness system can be linked with service access control equipment, such as an access control platform and security application gateway to perform identity authentication of equipment.

The situational awareness system has four types of awareness capabilities: awareness of basic security, system security, application compliance, and health status.

1) Basic security awareness refers to the ability to sense threats, such as viruses, APT attacks, and system vulnerabilities.
2) System security awareness refers to the ability to perceive risks related to login, account, configuration, and others.
3) Application compliance awareness refers to the ability to sense whether there is noncompliant software, processes, registry keys, and other risks.
4) Health status awareness refers to the ability to sense whether there are terminal risks related to browsers, file operations, and desktops.

The situational awareness system can identify the person operating a terminal through various physical environmental awareness devices, thereby identifying physical environment risks, such as UKEY plugging and unplugging, multiperson onlookers, and authorized personnel leaving.

TABLE I
RISK SCORING

Risk Setting	Description	Deduction Standard
Potential Risk	Low Risk Factor	0-10
General Risk	Medium Risk Factor	11-50
Severe Risk	High Risk Factor	51-100

4) Risk Judgment: Risk judgment includes two parts: risk scoring and risk reporting. The main purpose of risk scoring is to provide quick trust identification capabilities for 5G smart medical equipment. All security access strategies for smart medical services can be set based on the score. Main purpose of risk reporting is to provide in-depth terminal trust identification capabilities. All services can be judged based on specific attributes in the report for fine-grained access control of smart medical services.

Risk Scoring: The 5G smart medical situational awareness system adopts the principle of "trustworthy weighting," which adds up the weights generated by all risk items and presents them as percentages so that the strategy party can formulate corresponding security policies for different scoring results.

As for now, the situational awareness system uses an "awareness template" to define the credibility of the terminal, and the template can be customized by managers for their needs.

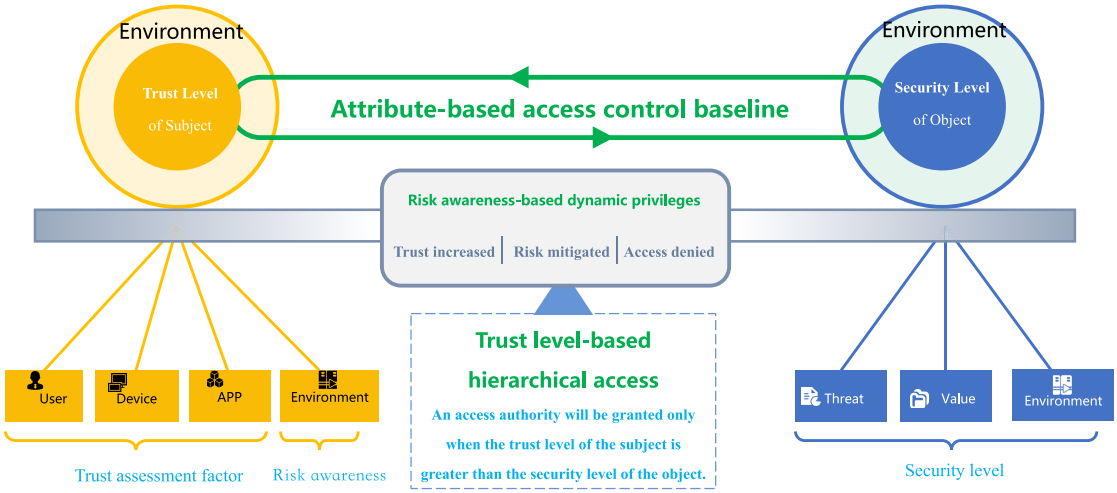

Fig. 3. Our access control model.

The terminal situational awareness system divides all awareness items into three levels: potential risk, general risk, and serious risk. The meaning and deduction criteria of these three types of risks are shown in Table I.

It adopts the initial 100-point system, in which detected risk items will result in the deduction of scores. The administrator can set different policy templates and metrics according to their needs. The terminal situational awareness system comprehensively perceives and measures the security status of the terminal from four aspects: awareness of basic security, system security, application compliance, and health status.

Risk Reporting: The 5G smart medical situational awareness system will form a risk report on the identified risk types and attributes and transmit it to the access control center. The access control center can bind specific attributes and services to achieve a fine-grained access control strategy.

C. Trust Assessment Model

The trust assessment model (shown in Fig. 2) is one of the core components of the ZTA that achieves continuous trust evaluation capabilities, the model is linked with the access control engine to continuously provide assessment data, such as trust level of subjects, security level of resources, and evaluation results of environment as the basis of deciding access control policies.

The trust assessment model is built on our 4D security framework of 5G smart medical care. It takes the smart medical personnel subject (i.e., attributes of user identity, credential security, and user behavior analysis), and the equipment subject (i.e., device identity attributes, terminal security status, and system behavior analysis) as inputs for the identity trust evaluation. The model conducts situational risk determination using the risk judgment mechanism (as described in Section III-B). It matches the object's security level with the subject's trust level. The discovery process of the behavioral dimension is continuously performed and reflected on the subject's trust evaluation.

The trust assessment model continuously performs trust evaluation, provides assessment results to the access control engine for decision-making operations of zero-trust strategies, determines whether access control policies needs to be changed, and interrupts connections through access agent in time to quickly perform resource protection if necessary.

During trust assessment processes, users are expected to develop quantitative standards to cope with their own security needs, and the standards may be refined during practices. Therefore, corresponding configuration interfaces should be reserved for such purposes.

The continuous dynamic assessment of ZTA should make full use of the existing security platforms as well as other security analysis platforms including security event management systems, threat intelligence systems, early warning and monitoring systems, and end-point protection systems. Those systems collectively provide asset status, regulatory requirements, security risks of operational environment, threat intelligence reports and other data to help the ZTA perform continuous and dynamic assessment.

D. Access Control Model

The access control model connects the control plane and the data plane and establishes access control policies for all access requests based on communication sessions from the data plane. As shown in Fig. 3, it comes up with basic access control privileges from security policies and basic trust levels. According to security contexts and the principle of "minimize access control," the model performs trust assessment continuously and adjusts access privileges dynamically. It implements dynamic access control policies strictly to block access requests without proper privileges.

Continuously receiving the assessment results from the trust assessment model and following the principle of least privilege, our access control model takes session as the basic unit and makes dynamic privilege judgments based on context attributes, trust levels and security policies for all access requests, and decides whether to grant permissions to resources access requests.

The data plane component of the ZTA is the policy enforcement point for dynamic access control capabilities.

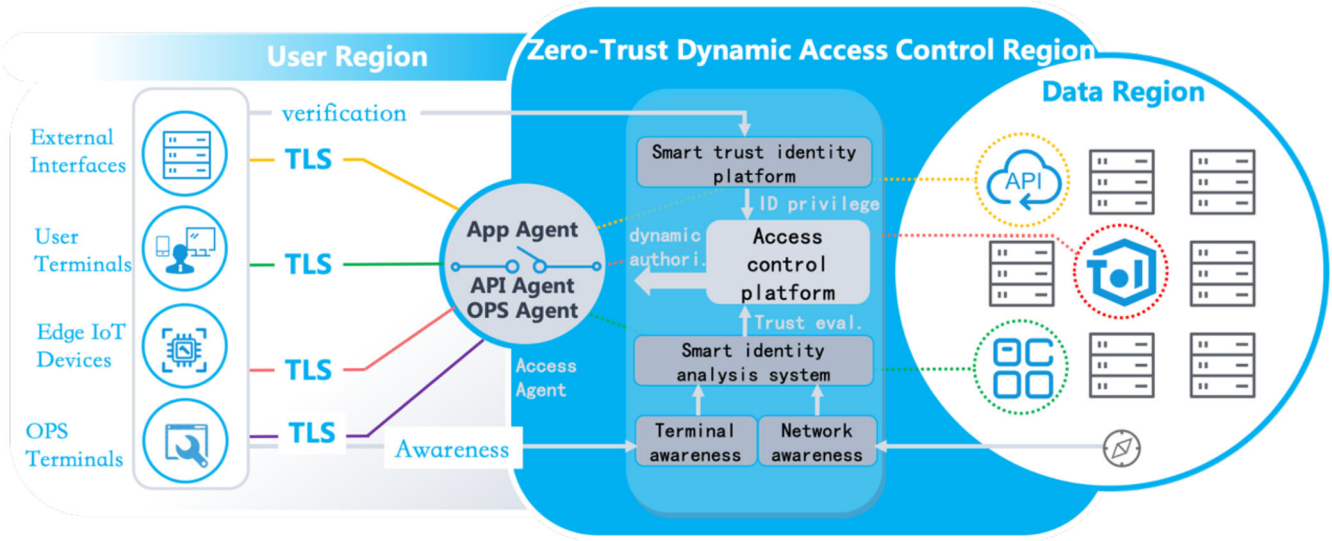

Fig. 4. Basic zero-trust security awareness and protection system architecture.

Once the access agent receives an access request, the access control engine authenticates the access subject and dynamically determines the authority of the access subject. Access agent will establish a secured channel for the access request that has passed authentication processes and has proper authority that allows the subject to access the protected resource. When access control engine determines that an established connection requires a policy change, access agent changes, suspends, or cancels the session accordingly.

IV. Zero-Trust Security Awareness and Protection System for 5G Smart Healthcare

ZTA was first proposed by National Institute of Standards and Technology in its special publication SP800-207 [25]. With the security principle of "never trust and always verify," the architecture processes data communications, authentications, and authorizations between involved entities. It consists of a control plane for communication control (e.g., session control), and a data plane for carrying application data. Subjects (e.g., clients) lodge their access requests on the control plane, which will then be handled by the trust assessment engine and access control engine for identity verification and authorization. Once an access request is approved, the system will configure the data plane dynamically, and access agent will receive communication data from subjects to establish one-time secured connections.

In the scenario of 5G smart healthcare, we propose an architecture of zero-trust security awareness and defence system. Driven by the 4D security framework (as explained in Section III) as well as the requirements of 5G smart healthcare, we enhance the proposed architecture in the aspects of virtualization, data collaboration, accessibility of IoT, and integrated 5G network security protection mechanism.

A. System Overview

The security awareness and protection system consists of 3 logical regions including user region, zero-trust dynamic access control region, and data region, as shown in Fig. 4.

1) User Region: The user region supports calling interfaces from external platforms, accessing services from user terminals, connecting IoT devices from the edge, and secured terminal access for operation and maintenance. All of the mentioned user region functionalities connect to the access agent via TLS.

2) Zero-Trust Access Control Region: The zero-trust access control region that is developed from the 4D security framework contains three key components including trust assessment engine, access control engine, and access agent.

Trust Assessment Engine: The trust assessment engine that contains the trust assessment model and the risk judgment mechanism in our 4D zero-trust security framework has the ability to continuously perform trust evaluation. It collaborates with the access control engine by continuously providing trust assessment grades of subjects, security assessment grades of resources, assessment results of network environment, and more, which are the basis of making access control strategies.

Access Control Engine: The access control engine that realizes the access control model in our 4D framework continuously receives assessment results from the trust assessment engine. It makes the ultimate decision on whether to grant permission to a request or not. By evaluating all requests, access to resources is granted on a per-session basis with least privilege principles and determined by dynamic policies on application content, levels of trust, and security policies.

Access Agent: Access agent is a component on the data plane, which executes the dynamic access control functionalities. On receiving access requests, the access agent performs identity authentication to make dynamic decisions on privileges of access. The agent establishes secured channels for verified subjects that hold proper privileges to access

protected resources. The access agent changes, terminates, or cancels a connection when the access control engine alters corresponding policies.

3) Data Region: Data region including cloud environment and edge is the storage and operational environment for access objectives. The access will be allowed into the data region once it passes evaluation and authorization in the zero-trust dynamic access control region.

B. Security Enforcement for Virtualized Networks

Applications of 5G smart healthcare adopt virtualization extensively. On the one hand, 5G networks are built on top of virtualized IT infrastructure, and use NFV technology for network slicing, which introduces security risks of virtualization into 5G communication networks and brings new attack surfaces; on the other hand, the fast-developing cloud and edge computing used in healthcare applications take advantages of open-source technologies. However, it also faces huge security threats due to the nature of open access for open-source code and libraries, which may be utilized by attackers. Potential consequences include accelerated attacks on container infrastructures and information leakages caused by vulnerabilities of containers.

Our security awareness and defence system for 5G smart healthcare apply zero-trust access control in a virtualized environment. It uses technologies that are compatible with could computing platform and makes sure that only workflows that are dynamically authorized can exchange and access data under continuous monitoring and control.

1) Fine-Grained Access Control: The fine-grained access control uses microsegmentation strategies that are applicable to virtualized components, such as virtual machines, containers, and microservices. It only allows data exchanges between authorized systems and connections, which are continuously updated by the fine-grained access control policies in the changing could environment. To be noted that, the microsegmentation strategies are not restricted by physical locations of virtual and dynamic assets.

2) Isolation Mechanism for Microservices: On using connection, security, control, and monitoring components provided by microservice management platform, our zero-trust system achieves application/service isolation, facilitates the development of core service logics, performs traffic monitoring, load matching, access control and auditing.

3) "Authenticate Before Connect" for Microservices: Our system authenticates accesses between microservices through identity-based verification and authorization. Once an authorization is obtained, two-way mTLS is used to encrypt the entire data link to achieve secured communication between clusters. Besides, minimized access control policies are applied in a self-adaptive manner.

C. Security Enforcement for Data Collaboration

While legacy security appliances are mainly designed for north-southbound (external) service models, the east-westbound (internal) data traffic generated by smart medical applications has increased significantly. Therefore, many problems occurred when legacy security solutions are deployed in the data center internally, such as difficulties in deployment, high computational overhead, and inflexible policy management. Our security awareness and protection system for 5G smart healthcare leverages microsegmentation technologies to achieve isolation of network environment, interdomain segmentation, and end-to-end segmentation, which are all adjusted in real-time according to events and changes of network conditions. Besides, other related security technologies, such as data encryption that are adopted in our system are not elaborated in this article for logical fluency and consistency.

1) Fine-Grained Segmentation of Security Policies: Our zero-trust system reduces network topologies by shutting down useless services in the network (e.g., removing inactive VLANs, subnets, network zones, or IP addresses). It also optimizes the policy creation process, sets access controls at boundaries of network zones with different security/trust levels, and establishes flat management for networks to realize delicacy management.

2) Identity-Based Logical Boundary: Our zero-trust system treats users, devices, and applications as access subjects, and performs identity authentication and security monitoring which are the trust basis of access control to ensure the trustworthiness of involved identities and devices. Besides, our system isolates connections between the visitors and internal resources of data centers, establishes fine-grained access control and prevents unauthorized access by the visitors.

3) Self-Adaptive Security Policies: Our zero-trust system is able to discover illegal internal traffic via analysis of access logic among services. It provides the basis for adjustments to security policies. When data canter experiences changes, corresponding security policies are automatically and quickly configured according to the calculation results provided by the policy analysis engine. Thus, our system significantly accelerates security workflows and reduces the risk of human error.

D. Security Enforcement for IoT Access

With the development of smart medical services, a smart medical platform faces the problem of hosting a large amount of IoT devices with various types and different connecting methods. Thus, to achieve effective and secure operations, it is necessary to manage accesses of those devices and servers uniformly. Considering the fact that connected IoT devices are huge in amount and weak in security capabilities, if proper measures are not in place, experienced attackers may exploit vulnerabilities of the connected devices to attack the platform from the inside, which leads to a higher risk.

Our security awareness and defence system for 5G smart healthcare employ a ZTA for IoT access. By using edge computing, it achieves identity verification and access control of terminals, grants access to trustable IoT devices that are authorized dynamically, monitors their behaviors at run-time, detects and handles fake or illegal connections promptly.

1) Deploying IoT Access Management Appliances at the Edge: Our system deploys access management appliances for IoT devices at the access edge for management purposes, such as identity management, privilege allocation, and access control. The appliances are linked with the data center to use its capability in computing, connection, and storage at the edge âĂŞ it enables our system to handle IoT-related requests with satisfying responsiveness and risk control.

2) Establishing an Identity Management Mechanism for IoT Devices: Different identities can be used in identity authentications for IoT devices with different characteristics to tackle the problems of terminal device and user identity counterfeiting. Identities of highly trustable devices are labeled by its trusted chips and OS. For embedded devices, device tags (e.g., IMEI, IDFA, and UDID), RFID electronic tags and password modules are helpful in establishing device identity. As for IoT devices with limited computational capability, device digital fingerprints can be used for network access identity management.

3) Constructing a Baseline Security Database for IoT Devices: Our system constructs a security baseline for IoT devices in a flexible manner. On the basis of IoT device identity management, our system obtains device information including types of operating systems, features of applications that touching sensitive data, service access logs and behavioral profiles, and constructs the security baseline library with the help of relevant techniques, such as machine learning and deep learning. It helps operators to quickly and accurately determine whether the operational environments of IoT devices are normal and to capture infected and malicious connected devices in time.

E. Integrated 5G Network Security

5G technology, that achieves network partitioning and application supporting via network slicing and edge computing, aggregates diversified applications into one network. However, its security requirements still hold diversity. Apart from the security risks already in 2G/3G/4G networks, the multiple dimensions of 5G network (e.g., could, edge and terminal) introduce more risks. With our zero-trust system, we solve the mobile communication network security, IT infrastructure security, and 5G smart medical application security as a whole. A unified 5G identity management mechanism, fine-grained user access control, and automatic configuration of access control policies are established ad hoc for the realization of an integrated 5G network awareness and security without modifying existing 5G core network architecture.

1) Constructing a Unified 5G Identity Management Mechanism: 5G network with applications is a huge ecosystem involving many security subjects, such as networking device vendors, operators, platform providers, security device vendors, and users. The 3GPP standard framework proposes security identification and authentication mechanisms, such as SUCI and AKA. Our system uses SUCI and AKA (encrypted from 5G users SUPI) to build an identity security management platform on the cloud or data centers in the core network. The platform achieves a unified multirole and scalable identity management, strong authentication methods, endpoint protection, authentication management as well as authentication and compliance of devices and (virtual) networks.

TABLE II
CONFIGURATION OF OUR TEST ENVIRONMENT

No.	Identity	Hardware	Software
1	Server	CPU: 40*2.4Ghz memory: 256G hard disk: 1TB + 4TB*12	OS: CentOS7.4 application: Spark2.3.1 database: MySQL
2	Client (PC)	memory: 16GB hard disk: 1024GB	OS: Windows10 browser: Chrome
3	Client (Phone)	Huawei	OS: Android 8 browser: Chrome
4	Client (Phone)	Apple	OS: iOS13 browser: Safari
5	Network	1000Mbps	

2) Realizing Fine-Grained User Access Control: The separation and isolation of the network and application layer of 5G network is easy to realize. Software-defined networking, the core technology of 5G network, enables an enterprise to achieve virtual networking, which makes it possible for the enterprise to flexibly construct and improve their network architecture on 5G infrastructure, and realize the separation and isolation of dynamic network security domains.

To achieve fine-grained security management and control, the security capabilities deployed on the 5G edge cloud are required, including the construction of a virtual access network with dynamic scheduling and elastic expansion, and a closed loop of awareness, analysis, and execution at the edge.

3) Automatic Configuration of Access Control Policies: The diversification and customization of 5G security needs require that the security capabilities are able to be quickly established and updated, and security components are able to be deployed in a distributed manner. Components are able to be adaptively adjusted and configured within the infrastructure and aggregated with information systems to enhance the ability to cooperation. Besides, an intelligent active defense is achieved by combining the unified identity management mechanism, the automatic configuration of security policies, and dynamic access control.

V. TEST AND EVALUATION OF THE ZERO-TRUST SECURITY AWARENESS AND PROTECTION SYSTEM

In order to verify the functional and real-time performance of the 5G smart medical security awareness and protection system leveraging ZTA, we set up an environment to test functions of each module and the overall operation of the system. The test was divided into two parts: 1) functionality test and 2) system performance test. The functionality test covered the functional modules at all levels to check whether the entire system meets the expected functional requirements. The system performance test demonstrated the ability to provide services after system integration, including reliability, safety, and maintainability.

A. Test Environment

According to the requirements of verification, we set up a test environment as shown in Fig. 5. All components (e.g.,

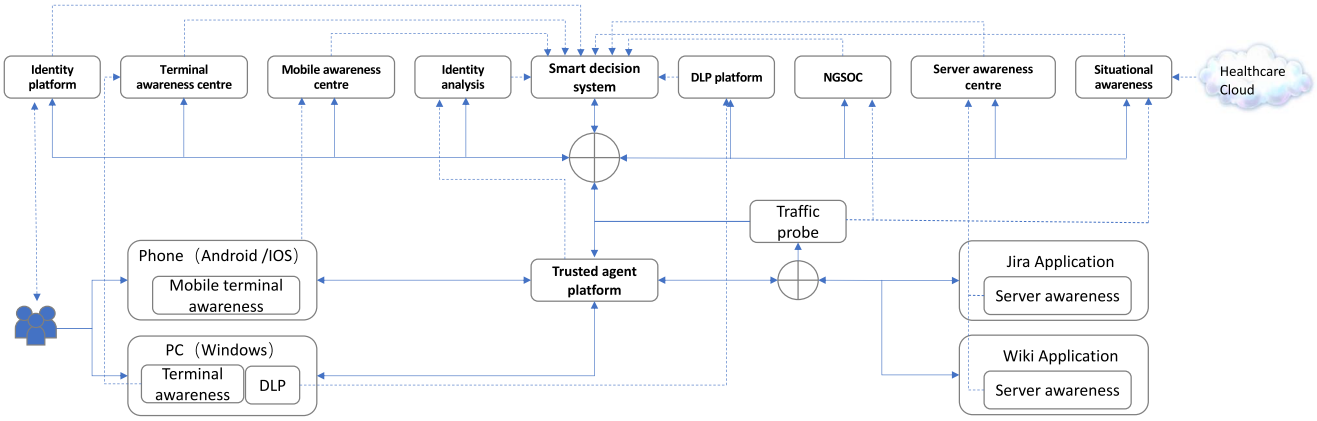

Fig. 5. Our test environment.

TABLE III
USER ACCESS BEHAVIOR ANALYSIS MODULE

No.	Test case	Expectation	Result	Status code	Error code
Unit test: Log receiving>>Data storage					
1	TAP logs are successfully stored in HIVE's noah database app_access.	Logs are stored successfully.	✓	◉	○
2	TAP logs are successfully stored in noah_app_access_yyyymmdd.	Logs are stored successfully.	✓	◉	○
Unit test: Peer group analysis>>Exception trigger					
3	Trigger exceptions for group-based user access.	The exceptions are triggered successfully.	✓	◉	○
4	Trigger exceptions for group-based user traffic requests.	The exceptions are triggered successfully.	✓	◉	○
5	Trigger exceptions for group-based user authentication.	The exceptions are triggered successfully.	✓	◉	○
Unit test: Pareto analysis>>Exception trigger					
6	Trigger individual-based user authentication exceptions.	The exceptions are triggered successfully.	✓	◉	○
7	Trigger individual-based user access exceptions.	The exceptions are triggered successfully.	✓	◉	○
8	Trigger individual-based user traffic exceptions.	The exceptions are triggered successfully.	✓	◉	○
Unit test: Unauthorized access analysis>>Exception trigger					
9	Trigger user unauthorized exceptions.	The exceptions are triggered successfully.	✓	◉	○
Unit test: User access behavior >>Exception trigger					
10	Trigger fraudulent account exceptions.	The exceptions are triggered successfully.	✓	◉	○
11	Trigger multiple login exceptions.	The exceptions are triggered successfully.	✓	◉	○
12	Trigger exceptions for multiple accounts on one device.	The exceptions are triggered successfully.	✓	◉	○
13	Trigger personal geographic location exceptions.	The exceptions are triggered successfully.	✓	◉	○
14	Trigger personal access time exceptions.	The exceptions are triggered successfully.	✓	◉	○
Unit test: User access behavior >>Credit calculation					
15	Abnormal behaviors are included in calculations of user credit.	All abnormal behaviors are included.	✓	◉	○
16	Each user will be deducted up to Z points for each type of abnormality.	Points are deduced as expected.	✓	◉	○
17	The minimum credit is 0 point.	The minimum credit is 0 point.	✓	◉	○
18	Successful timings for credit calculation.	Timings are successful.	✓	◉	○

servers, client terminals, and network capacities) used in the environment are at production grade and can be used in real practices.

Our test environment is the implementation of our system architecture (described in Section IV and visually presented in Fig. 4), which contains user region, access agent, zero-trust dynamic access control region, and data region. Mobile phones and PCs that are directly connected to the trusted agent platform are devices in the user region. Traffic probe, Jira, and Wiki applications that provide external interfaces are deployed and connected to the trust agent platform for situational awareness. The trusted agent platform acts as the access agent which works as the gateway for requests from the user region. In the zero-trust dynamic access control region, components including identity platform, terminal awareness centre, mobile awareness centre, and identify analysis interact with the smart decision system. As for data region components, DLP platform, NGSOC, server awareness centre, and situational awareness utilities are connected to the user region and access control region via switches.

Information from the various modules of our zero-trust system was gathered into the intelligent decision-making system for continuous trust assessment. Users PCs and mobile phones were connected to the trusted agent platform. And dynamic access control was then realized through an intelligent decision-making system. The configuration of our test environment is shown in Table II.

B. Functionality Test

Functional tests covered the functional modules of the entire system. The followings are the results of key modules.

1) User Access Behavior Analysis Module: Details of test cases and results for user access behavior analysis module are shown in Table III. Unit tests for key functionalities of user access behavior analysis module are presented, including log

TABLE IV
EQUIPMENT RISK ASSESSMENT MODULE

No.	Test case	Expectation	Result	Status code	Error code
Unit test: Functionality					
1	Obtain the tess template according to tpl_id and cache it to redis.	The template is obtained and cached.	✓	◉	○
2	The policy check item "Configuring Software Blacklist" is checked correctly according to the tess template.	Checked item is correct.	✓	◉	○
3	The policy check item "Configuring Software Whitelist" is checked correctly according to the tess template.	Checked item is correct.	✓	◉	○
4	The policy check item "install automatic vulnerability scanning tool" is detected correctly according to the tess template.	Checked item is correct.	✓	◉	○
5	The policy check item "Vulnerability Update Status" is detected correctly according to the tess template.	Checked item is correct.	✓	◉	○
6	The policy check item "Password Complex Policy" is checked correctly according to the tess template.	Checked item is correct.	✓	◉	○
7	The policy check item "Audit log size setting" is checked correctly according to the tess template.	Checked item is correct.	✓	◉	○
8	The policy check item "Audit log storage method" is checked correctly according to the tess template.	Checked item is correct.	✓	◉	○
9	The trust level of the device is calculated correctly.	Trust levels are calculated correctly.	✓	◉	○
Unit test: Exception					
10	No exception is thrown when getting address if the tess template is not configured.	No exception is thrown.	✓	◉	○
11	No exception is thrown when the tess template address is not found.	No exception is thrown.	✓	◉	○
12	No exception is thrown when tpl_id does not exist on the tess server.	No exception is thrown.	✓	◉	○

receiving, peer group analysis, Pareto analysis, unauthorized access analysis, and user access behavior analysis. The unit test for log receiving checks whether all system logs are stored in the database successfully; peer group analysis is designed to confirm that proper access control exceptions are triggered for abnormal group-based behaviors; Pareto analysis verifies that necessary access control mechanisms are enforced for individual-based illegal behaviors; unauthorized access tests whether correct access control exceptions are generated for unauthorized access behaviors; and tests for user access behavior demonstrate if the system can handle abnormal user access behavior and generate correct trust credits or not. All testing results are correct as expected with true value in status codes and null value in error codes.

2) Equipment Risk Assessment Module: Details of test cases and results for equipment risk judgment module are shown in Table IV. For this module, we performed unit tests for "functionality" and "exception." The tests for functionality validate security configurations are deployed correctly, and the test for exception shows how the system performs under abnormal status. It is clear that unit test results for both functionality and exception handling are as expected with proper status and error codes.

3) Trust Assessment Module: Details of test cases and results for trust assessment module are shown in Table V. In the evaluation of this module, we performed unit tests for its functionalities including calculation of trust baseline, calculation of trust model, operation of trust resolution strategy, and operation of trust push strategy. The tests for trust baseline calculation are developed to confirm that the configured security baselines can be correctly executed; the tests for trust model calculation verify the effectiveness of operations on the model; the tests for trust resolution strategy and trust push strategy validate the correctness of strategy configurations. All tests are passed with expected results.

4) Risk Decision Module: Details of test cases and results for risk decision module are shown in Table VI. Tests for this module verify the correctness of risk derivation, risk handling, and configurations of proper policies. Unit tests for its functionalities are performed, and all results are correct.

C. System Performance Test

System tests cover the operating environment and process of the entire system. Tables VII–IX illustrate key system test results for security, reliability, and maintainability, respectively. We present key test cases, testing processes, and results for the three aspects. The performance of our system meets design expectations and requirements.

D. Summary

As members of the project team, testers fully understood the services and functionalities of the system, therefore, they designed reasonable test plans and continuously tracked and tested our system at different stages during development and implementation. Our testers were allocated sufficient test utilities and resources according to our test plan. They tested the design, installation, implementation, and deployment of the system, and performed focused tests on key functional modules of the system. The overall operation of the system had also been systematically tested. The test results showed that the design and implementation of our project meet proposed expectations and can proceed to the next stage. However, with insights from the continuous operation of the system and onsite deployment of smart medical services, our system may

TABLE V
TRUST ASSESSMENT MODULE

No.	Test case	Expectation	Result	Status code	Error code
Unit test: Trust evaluation>>Trust baseline calculation					
1	Five levels of trust baseline can be customized.	The levels are customized successfully.	✓	◉	○
2	A diagram is generated for the baseline configuration of each level.	The diagram is generated successfully.	✓	◉	○
3	There is a corresponding illustrative figure when the number of each object is configured.	The figure shows the correct number of baseline objects.	✓	◉	○
4	Baseline configuration is effective.	Each object matches the baseline from low to high, and generates the corresponding baseline level.	✓	◉	○
Unit test: Trust evaluation>>Trust model calculation					
5	Modifications for each trust calculation model are enabled.	Modifications of the enable/disable status are successful.	✓	◉	○
6	The enabling and disabling of each trust computing model take effect.	The disabled trust models stop calculating, and the enabled trust models calculate normally.	✓	◉	○
Unit test: Trust assessment>>Trust resolution strategy					
7	Trust resolution strategy can be added, deleted, modified and queried.	Strategies are added, deleted, modified, and queried successfully.	✓	◉	○
8	Trust resolution strategy is effective within the set time.	Strategies are effective within the set time.	✓	◉	○
9	The trust resolution strategy can be set to be effective within a specified number of times.	Strategies match the set times.	✓	◉	○
10	The resolution strategy in effective can handle the corresponding trust query to the setting level.	Trust queries are handled successfully.	✓	◉	○
11	The setting level of the trust resolution strategy can be any level of [low-high].	Setting levels take effect.	✓	◉	○
12	Resolution strategy can be modified to enable/disable status.	The status is modified successfully and takes effect.	✓	◉	○
Unit test: Trust assessment>>Trust push strategy					
13	Trust push policy can be added, deleted, modified and queried.	Policies are added, deleted, modified and queried successfully.	✓	◉	○
14	Trust push policy can be modified to enable/disable status.	The status is modified successfully and takes effect.	✓	◉	○
15	The recipient of the push strategy can be any notification service in the TAC linkage configuration.	The recipient is successfully selected.	✓	◉	○
16	The object of the push strategy can be any object in the user/terminal/server/API.	The listed object is successfully selected.	✓	◉	○
17	The push strategy can push the trust change information of a specific object to a specific receiver.	The corresponding trust change is pushed successfully.	✓	◉	○

TABLE VI
RISK DECISION MODULE

No.	Test case	Expectation	Result	Status code	Error code
Unit test: Functionality					
1	Each individual risk derivation rule is added and matched correctly.	Rules are added and matched correctly.	✓	◉	○
2	Risk derivation rules under "&&" are added and matched correctly.	Rules are added and matched correctly.	✓	◉	○
3	Risk derivation rules under "||" are added and matched correctly.	Rules are added and matched correctly.	✓	◉	○
4	Risk derivation rules can be deleted.	Rules are deleted successfully.	✓	◉	○
5	The daily hit statistics of the risk treatment strategy are correct.	Statistics are correct.	✓	◉	○
6	The historical hit statistics of the risk treatment strategy are correct.	Statistics are correct.	✓	◉	○
7	After disabling an policy, it no longer takes effect.	The deactivated policy no longer takes effect.	✓	◉	○
8	After matching, correct contents are sent to the third-party address.	Contents are and sent correctly.	✓	◉	○
9	Modifications of the third-party address is effective.	Modifications take effect in the next epoch.	✓	◉	○
10	Modifications of the "action" in the policy become in effect immediately.	Modifications take effect immediately.	✓	◉	○
11	Deletions of a policy become in effect immediately.	The deleted policy no longer takes effect.	✓	◉	○
12	After matching, multiple policies are in effect.	Multiple policies take effect.	✓	◉	○

face pressures with the existing software and hardware configurations. As an example, the massive number of concurrent sessions within a single service may incur high computational costs during the continuous trust assessment process, and allocated resources for this service may be exhausted. Besides, as 5G infrastructures have not been maturely deployed in many cities, the computing power and network capability of each 5G node may not satisfy the operational requirements of 5G remote healthcare. Therefore, performance optimization and function adjustment with respect to those practical challenges are needed as future works.

VI. CONCLUSION AND DISCUSSION

In this article, we present a security awareness and protection system for 5G smart healthcare that leverages ZTA. Driven by the development of 5G smart healthcare and associated security challenges, we are the first to propose a 4-D

TABLE VII
SECURITY TEST

Test Case	Testing Process	Test Results
Verification of title privilege	Deploy userswitch.jsp and titletest.jsp to the corresponding applications; use these two files to test the privileges of all titles to ensure that different users can see the correct titles.	System permissions are set reasonably; and users with different privileges can see proper titles.
Verification of information ownership	Verify that the information of different users with the same title authority can only be operated by the authorized users, thereby ensuring the security and privacy of information.	Different users with the same authority of the system cannot perform illegal data operations.
Scanning of security vulnerability	Use vulnerability scanning tools to scan the entire system.	Use AppScan tool to scan; and result shows that it is safe.

TABLE VIII
RELIABILITY TEST

Test Case	Testing Process	Test Results
Maturity	When the used capacity reaches the specified limit, the system will not crash, exit abnormally, or lose data.	The system gives warnings when the limit is reached.
	When there is no enough capacity for current jobs, the system will not crash, exit abnormally, or lose data.	The system gives warnings when the limit is reached.
	The system will not crash or lose data when there are errors caused by other programs.	The system gives corresponding warning information.
	When entering illegal commands specified in the user documentation, the system will not crash or lose data.	The system gives a corresponding warning message, e.g., the format of the uploaded file does not meet the allowed format specification.
Fault tolerance	The system can avoid impacts of mis-operations from users.	Perform security checking of operations at the system level, take the date selection function as an example, the current date is used to prevents users from entering incorrect or invalid dates.
	There is corresponding warning information.	The system gives corresponding warning information.
	When entering wrong data, the system will not crash, exit abnormally, or lose data.	The system gives corresponding warning information.
	When there is an illegal operation, the system will not crash, exit abnormally, or lose data.	The system gives corresponding warning information.
Easy to recover	The system should be able to be recovered from failures quickly.	The system can be recovered quickly.
Data verification mechanism	The logical relationships between data items should be verified to ensure the validity of the data.	Data related operations are validated at the system level, such as verifying the start and end dates of an inserted data block to avoid errors.
	The integrity and consistency of the data should be guaranteed, and no junk data will be generated due to repeated data deletion or insertion.	Inserting and deleting data do not generate extra junks.
	For input data that does not meet the requirements, the system should provide concise and accurate prompt information and necessary helps.	Corresponding prompt information is given for illegal inputs.

TABLE IX
MAINTAINABILITY TEST

Test Case		Testing Process	Test Results
Graphical interface for various operations		1. Installation 2. Initialization 3. Use 4. Maintenance	Manuals for using the graphical interfaces are provided.
Customization of functions		Undertaking secondary development of functionalities using system interfaces.	Secondary developments are supported by a rich set of interfaces.
Maintainability of logs	Is there log?	Business operations can be automatically recorded in logs.	Operations in all modules of the system are recorded in logs.
	are logs traceable?	The content of logs should include: which user; when; which IP is used; which module to operate (to add address book, edit address book, or modify address book group, etc.); which business data (ID) is operated; and operation result (success of failure).	1. The system provides log operation and log management functions. 2. Can view the current latest log records, including date and time, IP address, operator, module name, summary, and query the corresponding log records based on collective conditions.
	Is log information correct?	All information contained in logs is recorded correctly. As an incorrect example, there is a failure that no result is given from executions, but this failure is missed in the log or not logged correctly.	All system log information is recorded correctly.

security framework for 5G smart healthcare considering four dimensions (i.e., subject, object, environment, and behavior). On the basis of this framework, we presented the architecture of our security awareness and protection system and discuss the achieved security enforcements for network virtualization, data collaboration, IoT access, and integrated 5G network

security to meet the security needs for 5G smart medical applications. Our system is implemented and tested thoroughly for its functionalities and performance.

We acknowledge that there are still many challenges for our zero-trust security awareness and protection systems in the scenario of 5G smart healthcare, such as difficulties in technical implementation and gaining public awareness. Yet there is no standard to assess the maturity of a security solution using ZTA, and the problems of incompatibility with existing security frameworks in the 5G smart medical industry still exist. Therefore, efforts from many aspects still need to be taken for the security awareness and protection system of 5G smart healthcare. As future works, we are conducting in-depth research and development of zero-trust-based security awareness and protection technologies on the top of our frameworks, models, and the system proposed in this article and making improvements according to feedbacks from practical deployments.

REFERENCES

[1] M. Agiwal, A. Roy, and N. Saxena, "Next generation 5G wireless networks: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 1617–1655, 3rd Quart., 2016.

[2] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, and M. Ylianttila, "Security for 5G and beyond," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3682–3722, 4th Quart., 2019.

[3] A. Akhunzada, S. U. Islam, and S. Zeadally, "Securing cyberspace of future smart cities with 5G technologies," *IEEE Netw.*, vol. 34, no. 4, pp. 336–342, Jul./Aug. 2020.

[4] R. Arnold and D. Longley, "Zero-knowledge proofs do not solve the privacy-trust problem of attribute-based credentials: What if alice is evil?" *IEEE Commun. Stand. Mag.*, vol. 3, no. 4, pp. 26–31, Dec. 2019.

[5] N. A. Azeez and C. V. der Vyver, "Security and privacy issues in e-health cloud-based system: A comprehensive content analysis," *Egypt. Informat. J.*, vol. 20, no. 2, pp. 97–108, 2019.

[6] A. Banchs, D. M. Gutierrez-Estevez, M. Fuentes, M. Boldi, and S. Provvedi, "A 5G mobile network architecture to support vertical industries," *IEEE Commun. Mag.*, vol. 57, no. 12, pp. 38–44, Dec. 2019.

[7] S. Buzzi, I. Chih-Lin, T. E. Klein, H. V. Poor, C. Yang, and A. Zappone, "A survey of energy-efficient techniques for 5G networks and challenges ahead," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 4, pp. 697–709, Apr. 2016.

[8] J. Cao *et al.*, "A survey on security aspects for 3GPP 5G networks," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 170–195, 1st Quart., 2020.

[9] M. Chen, J. Yang, J. Zhou, Y. Hao, J. Zhang, and C.-H. Youn, "5G-smart diabetes: Toward personalized diabetes diagnosis with healthcare big data clouds," *IEEE Commun. Mag.*, vol. 56, no. 4, pp. 16–23, Apr. 2018.

[10] L. Chettri and R. Bera, "A comprehensive survey on internet of things (IoT) toward 5G wireless systems," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 16–32, Jan. 2020.

[11] H. S. G. Pussewalage and V. A. Oleshchuk, "Privacy preserving mechanisms for enforcing security and privacy requirements in e-health solutions," *Int. J. Inf. Manag.*, vol. 36, no. 6, pp. 1161–1173, 2016.

[12] E. Gilman and D. Barth, *Zero Trust Networks: Building Secure Systems in Untrusted Networks*. Sebastopol, CA, USA: O'Reilly Media, 2017.

[13] R. Gupta, S. Tanwar, S. Tyagi, and N. Kumar, "Tactile-Internet-based telesurgery system for healthcare 4.0: An architecture, research challenges, and future directions," *IEEE Netw.*, vol. 33, no. 6, pp. 22–29, Nov./Dec. 2019.

[14] A. Gutmann *et al.*, "ZeTA-zero-trust authentication: Relying on innate human ability, not technology," in *Proc. IEEE Eur. Symp. Security Privacy*, 2016, pp. 357–371.

[15] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 196–248, 1st Quart., 2020.

[16] J. Kindervag, *No More Chewy Centers: The Zero-Trust Model of Information Security*, Forrester Res., Inc., Cambridge, MA, USA, 2016.

[17] A. Ksentini and P. A. Frangoudis, "Toward slicing-enabled multi-access edge computing in 5G," *IEEE Netw.*, vol. 34, no. 2, pp. 99–105, Mar./Apr. 2020.

[18] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 1, pp. 131–143, Jan. 2013.

[19] Q. Liu, T. Han, and N. Ansari, "Learning-assisted secure end-to-end network slicing for cyber-physical systems," *IEEE Netw.*, vol. 34, no. 3, pp. 37–43, May/Jun. 2020.

[20] D. Loghin *et al.*, "The disruptions of 5G on data-driven technologies and applications," *IEEE Trans. Knowl. Data Eng.*, vol. 32, no. 6, pp. 1179–1198, Jun. 2020.

[21] C. L. Ng, M. B. I. Reaz, and M. E. H. Chowdhury, "A low noise capacitive electromyography monitoring system for remote healthcare applications," *IEEE Sensors J.*, vol. 20, no. 6, pp. 3333–3342, Mar. 2020.

[22] J. Ordonez-Lucena, P. Ameigeiras, D. Lopez, J. J. Ramos-Munoz, J. Lorca, and J. Folgueira, "Network slicing for 5G with SDN/NFV: Concepts, architectures, and challenges," *IEEE Commun. Mag.*, vol. 55, no. 5, pp. 80–87, May 2017.

[23] S. Rose *et al.*, "Zero trust architecture," Nat. Inst. Stand. Technol., Gaithersburg, MD, USA, Draft (2nd) NIST SP 800-207, 2020.

[24] D. Rupprecht, A. Dabrowski, T. Holz, E. Weippl, and C. Pöpper, "On security research towards future mobile network generations," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 2518–2542, 3rd Quart., 2018.

[25] M. Samaniego and R. Deters, "Zero-trust hierarchical management in IoT," in *Proc. IEEE Int. Congr. Internet Things (ICIOT)*, 2018, pp. 88–95.

[26] S. Sengupta and S. S. Bhunia, "Secure data management in cloudlet assisted IoT enabled e-health framework in smart city," *IEEE Sensors J.*, vol. 20, no. 16, pp. 9581–9588, Aug. 2020.

[27] M. A. Simplicio, L. H. Iwaya, B. M. Barros, T. C. M. B. Carvalho, and M. Näslund, "SecourHealth: A delay-tolerant security framework for mobile health data collection," *IEEE J. Biomed. Health Informat.*, vol. 19, no. 2, pp. 761–772, Mar. 2015.

[28] S. Su, Z. Tian, S. Liang, S. Li, S. Du, and N. Guizani, "A reputation management scheme for efficient malicious vehicle identification over 5G networks," *IEEE Wireless Commun.*, vol. 27, no. 3, pp. 46–52, Jun. 2020.

[29] Y. Tao, Z. Lei, and P. Ruxiang, "Fine-grained big data security method based on zero trust model," in *Proc. IEEE 24th Int. Conf. Parallel Distrib. Syst. (ICPADS)*, 2018, pp. 1040–1045.

[30] A. Vergutz, G. Noubir, and M. Nogueira, "Reliability for smart healthcare: A network slicing perspective," *IEEE Netw.*, vol. 34, no. 4, pp. 91–97, Jul./Aug. 2020.

[31] X. A. Wang, J. Ma, F. Xhafa, M. Zhang, and X. Luo, "Cost-effective secure e-health cloud system using identity based cryptographic techniques," *Future Gener. Comput. Syst.*, vol. 67, pp. 242–254, Feb. 2017.

[32] Y. Xiao, Y. Jia, C. Liu, X. Cheng, J. Yu, and W. Lv, "Edge computing security: State of the art and challenges," *Proc. IEEE*, vol. 107, no. 8, pp. 1608–1631, Aug. 2019.

[33] Z. Zaheer, H. Chang, S. Mukherjee, and J. Van der Merwe, "eZtrust: Network-independent zero-trust perimeterization for microservices," in *Proc. ACM Symp. SDN Res.*, 2019, pp. 49–61.

[34] X. Zhang, A. Kunz, and S. Schröder, "Overview of 5G security in 3GPP," in *Proc. IEEE Conf. Stand. Commun. Netw. (CSCN)*, 2017, pp. 181–186.

[35] B. Zimmer, "LISA: A practical zero trust architecture," in *Proc. Enigma*, Santa Clara, CA, USA, Jan. 2018.

Baozhan Chen received the M.S. degree from the College of Information Engineering, Northwest A&F University, Xianyang, China, in 2014.

He is an Engineer of Medical Informatization with the National Engineering Laboratory for Internet Medical Systems and Applications of China, Zhengzhou, China, the National Telemedicine Center of China, Zhengzhou, and the First Affiliated Hospital of Zhengzhou University, Zhengzhou. His current research interests include 5G, Internet of Things, medical informatization, network security, system test, and medical artificial intelligence.

Siyuan Qiao received the B.S., M.S., and Ph.D. degrees in mathematics (information security) from Shandong University, Jinan, China, in 2003, 2007, and 2010, respectively.

He was in research of cryptography with the Institute of Advanced Studies of Tsinghua University, including differential attacks on international crypto algorithm standard SHA-1, and preliminary research on China's commercial crypto standard SM3. He is currently the Deputy Chief Engineer with Qi An Xin Technology Group Inc., Beijing, China, research on frontier field of cyber security, such as 5G, IoT, and blockchain. Leading a 5G & IOT security working group.

Jie Zhao received the Ph.D. degree in management science and engineering from Wuhan University of Technology, Wuhan, China, in 2008.

He is a Professor and a Doctoral Supervisor with the First Affiliated Hospital of Zhengzhou University, Zhengzhou, China. He is the Director of the Telemedicine Informatization Professional Committee of Chinese Health Information and Big Data Association, the Director of the Clinical Pharmacy Branch of Chinese Medical Association, and the Executive Vice President of the Chinese Health Internet+ Telemedicine Alliance. He is also the Director of National Telemedicine Center, Zhengzhou, China, National Engineering Laboratory for Internet Medical Systems and Applications, Zhengzhou, and Henan Engineering Research Center of Digital Medicine, Zhengzhou. He is one of the academic leaders in medical informatization, telemedicine, and clinical pharmacy in China. He has published more than 80 academic papers, six academic works, and 15 national software copyrights. He has presided over 21 national and ministerial projects, including the National Key Research and Development Program of China, National Natural Science Foundation of China. His research interests mainly include medical health information management and security for 5G smart healthcare.

Dongqing Liu received the B.Sc. and M.Sc. degrees from Jilin University, Changchun, China, in 2011 and 2014, respectively, and the Cotutelle Ph.D. degree from the University of Montreal, Montreal, QC, Canada, and the University of Technology of Troyes, Troyes, France, in 2019.

He is currently a Researcher with the National Engineering Laboratory for Internet Medical Systems and Applications, Zhengzhou, the First Affiliated Hospital of Zhengzhou University, Zhengzhou, China. His research interests include cloud computing, mobile-edge computing, Internet of Things, and smart healthcare.

Xiaobing Shi received the B.Sc. and M.Sc. degrees in control science and engineering from Shandong University, Shandong, China, in 2016 and 2019, respectively.

She currently works with the National Engineering Laboratory for Internet Medical Systems and Applications, Zhengzhou, and the First Affiliated Hospital of Zhengzhou University, Zhengzhou, China. Her research interests include 5G, Internet of Things, and smart healthcare.

Minzhao Lyu received the B.Eng. degree (First Class Hons.) from the University of New South Wales, Sydney, NSW, Australia, in 2017. He is currently pursuing the Ph.D. degree in computer networks with the University of New South Wales and CSIRO's Data61, Sydney.

He is currently a Research intern with the National Engineering Laboratory for Internet Medical Systems and Applications, Zhengzhou, China, the National Telemedicine Center of China, Zhengzhou, the First Affiliated Hospital of Zhengzhou University, Zhengzhou, where he contributed to this work. His research interests include programmable networks, network security, and applied machine learning.

Haotian Chen received the B.Sc. degree in electrical and electronic engineering from Washington State University, Pullman, WA, USA, in 2015, and the M.Eng. degree in electrical and electronic engineering from the University of Sheffield, Sheffield, U.K., in 2016.

He currently works with the First Affiliated Hospital of Zhengzhou University, Zhengzhou, China. His current research interests include telemedicine, e-health, 5G intelligence healthcare, and big data.

Huimin Lu (Senior Member, IEEE) received the B.S. degree in electronics information science and technology from Yangzhou University, Yangzhou, China, in 2008, the M.S. degree in electrical engineering from the Kyushu Institute of Technology, Kitakyushu, Japan, and Yangzhou University in 2011, and the Ph.D. degree in electrical engineering from the Kyushu Institute of Technology in 2014.

He is currently an Excellent Young Researcher of MEXT, Tokyo, Japan. His current research interests include computer vision, robotics, artificial intelligence, and ocean observing.

Yunkai Zhai received the Ph.D. degree in management science and engineering from Wuhan University of Technology, Wuhan, China, in 2008.

He is a Professor and the Doctoral Supervisor with Zhengzhou University, Zhengzhou, China. He serves as the Director of the Engineering Laboratory of Henan Province for Internet Medical E-commerce and Active Health Services, the Deputy Director of the National Telemedicine Center, the Deputy Director of the National Engineering Laboratory for Internet Medical Systems and Applications. He is one of the academic and technical leaders in the field of medical information system and management in China. He has undertaken 16 projects and published more than 120 papers and two national industry standards. He has won 21 software copyrights, published eight monographs and won seven provincial science and technology progress awards. His research interests mainly include medical health information management and security for 5G smart healthcare.