Hindawi
Security and Communication Networks
Volume 2022, Article ID 2509267, 13 pages
https://doi.org/10.1155/2022/2509267

Research Article

Risk-Based Dynamic Identity Authentication Method Based on the UCON Model

Jing Liu,[1,2,3] **Rongchao Liu**,[1] **and Yingxu Lai**[1,3]

[1]*College of Computer Science, Faculty of Information Technology, Beijing University of Technology, Beijing 100124, China*
[2]*Shaanxi Key Laboratory of Network and System Security, Xidian University, Xi'an 710071, China*
[3]*Engineering Research Center of Intelligent Perception and Autonomous Control, Ministry of Education, Beijing 100124, China*

Correspondence should be addressed to Yingxu Lai; laiyingxu@bjut.edu.cn

Received 17 December 2019; Accepted 16 November 2020; Published 31 March 2022

Academic Editor: Kaitai Liang

With the continuous progress of computer technology, static identity authentication technology has encountered challenges in practical applications; in addition, it has deficiencies in continuity and mutability. For these reasons, we propose a risk-based dynamic identity authentication method based on the Usage Control (UCON) model. When authenticating a user, we consider their access rights based on the degree of risk, except in case of password authentication. We propose a risk assessment method, and blockchain technology is used in the scheme to provide a reliable process for risk assessment and authorization. Our scheme represents an improvement in traditional identity authentication, resulting in higher continuity and mutability. We also prove that the scheme has high security and scalability.

1. Introduction

With the ongoing progress of Internet technology, the number of Internet users continues to grow rapidly. According to a report from the National Science Foundation [1], the number of global Internet users will increase to five billion by 2020. Despite the conveniences that the Internet brings to people's lives, there are also a number of serious problems. Internet sharing threatens the security of user information [2]. One of the most serious problems is hacker exploitation of a user's digital identity. Impersonation of a user by guessing or stealing their authentication credentials is the most common Web application attack [3]. During May–June 2018, more than 8.3 billion malicious login attacks have occurred on Akamai's Intelligent Edge Platform [4]. In order to protect website resources, it is important to take affirmative measures to verify digital identities. However, traditional authentication has not adapted well to the current network environment. It has been reported that in December 2018, attackers were able to bypass the two-factor authentication provided by services such as Gmail and Yahoo! Mail [5]. With the study of trust management in the modern network [6–8], it can be observed that traditional identity authentication still has weaknesses [9]. It mainly has the following problems:

(a) Lack of continuity and flexibility: existing methods mostly rely on a user's deterministic credentials or characteristics. When the system authenticates the user, it is often based on the credentials provided by the user at a certain moment but not on the previous behavior of the user.

(b) Inability of the identity authentication center to guarantee its own security and credibility, which it should be able to do as the trusted third party. For example, when the authentication center is attacked, users' identity information may be exploited or tampered with.

1.1. Motivation. The purpose of our scheme is to implement a more secure and accurate method of verifying a user's digital identity in order to protect sensitive information and maintain network security. Therefore, based on the Usage

Control (UCON) model [10], our scheme proposes a risk-based dynamic identity authentication method using blockchain technology to improve security via a decentralized network environment. Our scheme has not only a particular theoretical significance in the field of cryptography and information security but also important application value for the new e-commerce.

Our scheme provides improvements, namely, more flexible and secure website identity authentication. The main contributions of our study are as follows:

(a) When a user requires authentication, we refer to the user's password authentication and access control. These results determine whether the user is authenticated.

(b) The user's risk value emerges from an assessment of their historical behavior. In the risk assessment step, we propose a risk value calculation method.

(c) A user's information is saved in the blockchain to enhance security. Furthermore, we use smart contracts to control the user's access. In this way, we improve the security of the authentication process.

The remainder of this paper is organized as follows. National and international research in this field is introduced in the Related Works section. The section Materials and Methods introduces our risk-based dynamic identity authentication method. Security analysis and performance evaluation are presented in the section Results and Discussion. Our summary is provided in the Conclusions section.

2. Related Works

In this section, we first introduce the research of different identity authentication methods by domestic and foreign scholars. Subsequently, this paper presents blockchain research in the field of identity authentication and access control.

2.1. Identity Authentication. RFC 2828 [11] defines a user's identity authentication as the process of verifying the identity declared by the system. It is recognized that a secure and effective identity authentication should have the following features to meet the needs of users: first, it can protect users from being attacked; second, it should be capable of protecting privacy; third, it needs to be scalable; lastly, it should be user-friendly. To satisfy the demands created by these four converging trends, a number of authentication methods have emerged. Identity authentication methods can be segmented into three types:

(a) Verify your identity based on the information you know (what you know)

(b) Prove your identity based on what you have (what you have)

(c) Use unique physical characteristics to prove your identity (who you are) [12]

Password verification is the most common example of "what you know." Its method of verification is relatively simple compared with the others; therefore, it is usually considered to be the weakest link in the modern information chain. People rarely use password verification alone but often combine it with other methods.

"What you have" depends on what items people use to prove their identity. For example, smart cards. In combination with verification, it can improve the security of identity authentication. Yang et al. [13] developed the smart card password authentication method of Song [14] in 2014. They used a random number instead of a timestamp and protected the password with a one-way hash function. However, their methods are computationally complex, so an attacker can perform clogging attacks with a valid ID, leading the server to spend a lot of time doing useless calculations. Jangirala et al. [15] proposed a smart card authentication method based on a dynamic ID. Users can freely choose their login credentials and regenerate passwords with smart cards at any time. However, due to the high dependence on smart cards, a user's account will face a high risk if the smart card is lost. Considering the cost of replacing the smart card, this method is less scalable.

The identity authentication method of "who you are" is more reliable than traditional password authentication. Odelu et al. [16] proposed a multiserver authentication protocol based on secure biometric technology with smart cards. In their scheme, the registration center authenticates the user and the server separately when a secret key is established. It also supports revocation and reregistration. While this approach resists many logged-in user attacks, it still faces problems, such as the theft of smart cards, and will face risks if the registry is attacked. In He's method [17], a multiserver environment authentication scheme is proposed based on robust biometrics. The scheme does not use smart cards and protects user information from attacks to some extent. However, the capturing of a user's biometric information in the system database cannot be undone. Sun et al. [18] proposed a lightweight multifactor authentication method. This project is a combination of user biometrics and the information on a smartphone. With this method, they can achieve mutual authentication between the user and the remote server. However, this scheme does not save a fixed biometric template. Challa et al. [19] proposed an efficient ECC-based provably secure three-factor user authentication and key agreement protocol; however, it increases the computational and communication costs.

In summary, the identity authentication method of "what you have" depends on what is held by users; once it is stolen (i.e., identity theft), it will be at risk. "Who you are" depends on the characteristics of authentication but has the problem of high cost and a complicated process. In addition, because these methods are all static, they cannot adapt well to the complex and variable network environment.

With the development of network technology, some scholars [20–23] began to explore new authentication methods in order to adapt to the changing network environment [24]. In 2013, in the RSA "Risk-Based Authentication" white paper [25], a risk-based authentication system

that applies a user's risk analysis to identity authentication methods was described. Risk analysis and assessment can be used to identify risks in information assets to protect from threats. Luo et al. [26] designed a network information security risk assessment model based on an improved backpropagation neural network. They used the rough set attribute reduction method to reduce various factors affecting network and information security and to assess risk. However, the scheme does not differentiate between the risks involved, making the evaluation incomplete. Patil [27] performed a fault tree analysis based on two security events. However, the solution did not consider risk dynamics. It is necessary to reflect the changing tendency of threats in risk assessment with the changing network [28]. Risk-based authentication is a dynamic authentication system that takes the risk scores of the user who accesses the system into account. It is based on the method of "what you do," providing a new means of identity authentication. However, the authentication process in this scheme is complicated and the method of assessing risk is inadequate; thus, further improvements are needed.

2.2. Application of a Blockchain in Identity Authentication and Authority Control. Other scholars began to explore the combination of new network technology and identity authentication [29–31]. Among these technologies, blockchain was given particular attention. Blockchain is a new application mode of distributed data storage, point-to-point transmission, consensus mechanisms, and encryption algorithms [32]. With blockchain entering the 2.0 era, its high security and high expansion have opened up a new space for research in the field of network security [33, 34]. Some studies have proposed applications for the financial function of the blockchain (e.g., digital cryptocurrency). Sanda and Inaba [35] have studied methods for solving authentication problems related to Wi-Fi. They chose digital currency as the identity credential. When the user logs in, he can pass the identity authentication if he has Authcoin™. Jangirala et al. [36] have designed a secure lightweight blockchain-enabled RFID-based authentication protocol for supply chains in order to improve the safety of the 5G mobile edge computing environment. Raju [37] has investigated Ethereum's anonymous account wallet that not only manages a user's identity through public key addresses but also performs network authentication and payment functions by smart contracts. Other scholars have focused on constructing an access mechanism based on blockchain technology that allows legitimate users to access system resources but prohibits unauthorized user access. Cruz et al. [38] integrated blockchain as a role-based access control (RBAC) model to solve interorganizational access problems in RBAC, achieving cross-organizational authentication. Dorri et al. [39] applied blockchain to the smart home. They stored access control strategies in a blockchain and assigned privileges through blockchain transactions in order to handle all communications of the home. Zyskind et al. [40] described a decentralized personal data management system. They implemented a protocol that can transform a blockchain into an automatic access control manager. However, the current mainstream blockchain consensus mechanism is based on computing power; running a blockchain separately to provide access control services would be too costly.

Smart contracts [41] are scripts running automatically on a blockchain. They are a "transaction agreement that enforces contracts through a computer." Azaria et al. [42] achieved access control of medical data with the help of smart contracts based on Ethereum. They proposed the MedRec framework that combines smart contracts with access control, enabling the integration of distributed medical data and permissions. Ramachandran [43] used smart contracts and the Open Provenance Model to record immutable data paths and the changes in data for collecting trusted data sources.

Blockchain is a technology that guarantees the integrity of data through an immutable distributed ledger. Its chain structure and consensus mechanism characteristics are very important in maintaining the integrity of network data. The distributed domain name service provided by blockchain helps alleviate the current DNS vulnerability, which is beneficial in improving network system security [44]. Based on the above characteristics, blockchain should be more fully applied in the field of identity authentication, which will provide a new means for constructing a trusted relationship in cyberspace. In addition, a blockchain platform based on smart contract operation, for example, the hyperledger fabric, can run in a partially trusted environment with low cost, low latency, and low bandwidth density. Therefore, it is suitable for small and medium-sized networks [45]. However, in private and consortium blockchains, it is necessary to ensure the authenticity of the node's identity. Too strong anonymity will leave user resources more vulnerable to attackers.

To summarize, traditional identity authentication methods have various flaws, and authentication based on a user's risk behavior can improve flexibility. Nonetheless, due to the high security, low cost, low latency, and low bandwidth density of the consortium blockchain platform based on smart contract operation, if it is used for identity authentication in a medium-sized network on the basis of ensuring efficiency, it will improve reliability and security.

3. Materials and Methods

In this section, a risk-based dynamic identity authentication method is proposed, which locates the network on a campus. In order to adapt to the complex and changeable characteristics of a modern network, we make improvements to the UCON model. In addition, in order to provide a reliable process of risk assessment and authorization, blockchain technology is used in our scheme. Continuity and mutability are the keys of our scheme and high security and reliability.

The basic framework consists of three parts—client, identity authentication server, and blockchain. Its structure is shown in Figure 1. Our program consists of six phases: ① Initialization. In this step, the parameters required for the subsequent process are created. ② Registration. A user's

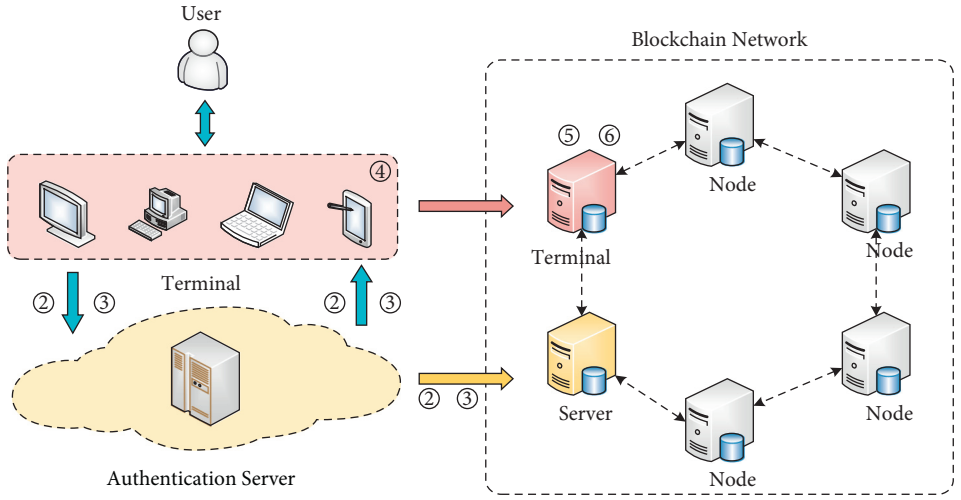

Figure 1: Structure of the scheme.

identity will be registered in our system in this step. ③ Authentication. The server authenticates the user when he requests access. ④ User access to resources. After a successful login, the user can access the website resources. ⑤ Risk assessment. In this phase, risk assessment is conducted for risk behavior. ⑥ Authority control. At this stage, the user's related information is stored in a blockchain, and the user's access right is controlled by smart contracts. Next, we will elaborate on these steps.

3.1. Initialization. In this step, the system will generate a cryptographic key k and a timestamp T for communication, a one-way hash function H to protect sensitive user information, and a security parameter λ for the signature process.

3.2. Registration. Users should register their identity to the server for further action. The primary operations are as follows:

The identity information consisting of the user's ID, password psw, and the timestamp T is encrypted by k; then, they are transmitted to the server S.

After receiving the user's message, the server first verifies the cryptographic key k with cipher-based message authentication code (CMAC) [46], then calculates the difference between the current time and the timestamp to verify the timestamp T. If the verifications are all correct, the user's registration information will be extracted.

The server converts the user's sensitive information into a fixed-length hash code with the hash function H and saves it securely.

The server generates a system signature public key Pu and a system signature private key Pr [47] according to the user's ID, password psw, and the security parameter λ.

The server converts the user's ID to his pseudonym $ID*$.

The server uses Pr to sign and obtain the signature Θ of $ID*$.

The server sends $ID*$ and the user's related information and timestamp T through a secure channel provided by a blockchain.

The blockchain stores the initial right A of the user. For a new user who has not yet accessed, we trust by default and provide a corresponding access right according to the user's identity.

The server returns a successful registration message to the user.

This process is shown in Table 1.

3.3. Authentication. A user must be authenticated before accessing resources. Our scheme refers to the results of password authentication and access right. The primary operations are as follows.

The user inputs their ID and password. Since the password is entered during login, we are uncertain whether the entered value is consistent with the stored one. In order to distinguish it from the password saved in the server, we use psw' to represent the login password. Then, the encrypted passwords, newly entered and stored, and the timestamp T are transmitted to the server.

After receiving the message from the user, the server first verifies the cryptographic key k and the timestamp T as in the registration step. If they are both correct, the user's login information can be obtained.

The server compares H (ID, psw) and H (ID, psw') to verify if ID and psw' are equal to the stored values. If the verification is consistent, it indicates that the password authentication is successful, and then the authority verification will be taken; otherwise, the server returns a failure message Fal.

The server sends a query request Req to the blockchain for authority verification. When receiving the access right from the blockchain, the signature verification algorithm is executed to verify the correspondence between ID and $ID*$. If the validation is successful, it means that the pseudonym $ID*$ belongs to ID.

The server reads the results from the blockchain. If the query result is "*accessible*," it indicates that the identity authentication succeeds; otherwise, the authentication fails. The authentication result will be sent to the user.

Table 1: User's registration process.

User (U)	Server (S)	Blockchain (B)
Input *ID*, *psw* Choose T Encrypt the message with k $\{T, ID, psw\}\ k$ ⟶		
	Decrypt k Verify whether T is correct *Get ID*, *psw* Save H (*ID*, *psw*) safely Calculate (Pu, Pr) Calculate $ID*$ Sign Sig $(ID*) \longrightarrow \Theta$ $\{T, ID*, \text{etc.}\}$ Secure channel ⟶	Generate initial right A based on risk Save ($ID*$, etc., A)
	Return registration success information $\{T, Suc\}\ k$ ⟵	

This process is shown in Table 2.

3.4. User Access to Resources. After being verified, the user can access resources on the website. Session [48] can be used to store information throughout the user's visit. When moving from one page to another, the visit record will be stored in a Session Object. With the help of the Session, we can identify a single session of the user and record related information in the process of one visit (login ⟶ access ⟶ logout) throughout the website.

3.5. Risk Assessment. At this stage, the user's future risk will be predicted based on their existing operations. In our scheme, we judge the qualitative risk [49] of the user. The main elements of qualitative risk are asset value, vulnerability, and threat. Based on these elements and the duration and frequency of a user's risky behavior, we can calculate a user's risk value and trust value.

In this study, a user's access to a campus network is taken as an example to describe how to calculate the risk. The resource value, vulnerability, and user's risk behavior can be divided according to the definition of risk factors in the risk assessment specification for information security (GB/T 20984-2007) [50]; these are shown in Tables 3–5.

According to the risk equation for information security, a user's risk value F can be expressed as follows:

$$F = W \times L \times R, \tag{1}$$

where W is the value of the resource, which is shown in Table 3 and describes the different types of resources and the importance of the resource; L represents the level of vulnerability, which is shown in Table 4 and describes the damage of the vulnerability; R represents the harm degree of the risk behavior to the system, which is shown in Table 5.

However, the calculated value is too large and unsuitable for us to describe the trend of risk changes. In order to evaluate the risk more conveniently, we can quantify it as follows:

$$F = \sqrt[3]{W \times L \times R}. \tag{2}$$

According to equation (2), we can obtain the user's risk at a certain moment, that is, the user's static risk. However, we consider that a user's behavior is not fixed, so their risk should also be dynamic. Therefore, combining the frequency and duration of a user's risk behaviors, the user's risk value can be expressed as follows:

$$F = \begin{cases} \theta \times F_0 \text{ (a)}, \\ F_0 + e^t \times \sqrt[3]{W \times L \times R} \times \dfrac{M}{Ti} \text{ (b)}, \end{cases} \tag{3}$$

where F is the user's risk.

Equation 3(a) describes the attenuation process of the user's risk value when a user behaves normally; θ is the risk attenuation factor, which is a constant less than 1; F_0 is the user's last risk value. It can be seen that when the user behaves normally, their risk is attenuated gradually and slowly.

Equation 3(b) reflects the increasing trend of the risk value when the user has risky behavior. In this formula, t represents the duration of a user's risky behavior and M/Ti represents the frequency of these behaviors. It can be seen that the risk value increases with the frequency and duration of the user's risk behavior, and it increases sharply.

In order to increase the accuracy, we measure the access rights of users according to their trust value. We can calculate a user's trust value Tr by the user's risk value as follows:

$$\text{Tr} = \begin{cases} \text{Tr}_0 - P^{(F-F^*)} & \left(F > F^*\right) \text{ (c)}, \\ \text{Tr}_0 + \dfrac{F^* - F}{q} & \left(F < F^*\right) \text{ (d)}, \end{cases} \tag{4}$$

Table 2: Authentication.

User (U)	Server (S)	Blockchain (B)
Input ID, psw' Choose T Encrypted message with k $\{T, ID, psw'\}$ k ⟶		
	Decrypt k Verify whether T is correct Calculate $H(ID, psw)? = H(ID, psw')$ No, return a wrong message $\{T, Fal\}$ k ⟵ $\{T, Req\}$ ⟵ Secure channel	
		Return access right $\{T, ID*, A\}$ ⟵ Secure channel
	Verify ID consistency $(ID, ID*, \Theta)? = 1$ Yes Verify whether A is accessible Yes $\{T, Suc\}$ k ⟵ No $\{T, Fal\}$ k ⟵	

Table 3: Resource value level of the campus.

Importance	Value	Type	Introduction
V	80–100	Infrastructure	Server pool composed of computing nodes; will cause very serious damage if destroyed
IV	60–80	System resources	Website's operating systems; will cause serious damage if destroyed
III	40–60	Shared data	Data that need to be shared; will cause some damage if destroyed
II	20–40	Application tool	Auxiliary application on the website; will cause loss after being destroyed
I	0–20	Portal information	Announcements; causes almost no damage if destroyed

Table 4: Level of vulnerability.

Level	Value	Extent	Introduction
V	80–100	Very dangerous	Vulnerabilities that access system permission directly
IV	60–80	Dangerous	Sensitive information is leaked or visited without authorization
III	40–60	Moderately dangerous	Causing Web application denial of service
II	20–40	Slightly dangerous	Causing denial of service locally or leaking general information
I	0–20	Almost safe	General CSRF or URL jumping

Table 5: Level of risk behavior.

Level	Value	Type of behavior	Introduction
IV	75–100	Malicious security behavior	Attack system through a virus or Trojan horse; may cause very serious damage
II	50–75	Behavior of breaking a contract	Unauthorized operation may affect the normal operation of the system
I	25–50	Abnormal behavior	Includes abnormal operation, abnormal access content, etc.; does a little harm to the system
I	0–25	Abnormal condition	Includes abnormal login location, abnormal equipment, etc.; has almost no impact on the system

where Tr represents the user's trust value, Tr_0 is the last one, F is the user's risk value, and F^* is the user's risk threshold.

Equation 4(c) represents the process of reducing the trust value when the user's risk value exceeds the risk threshold; P is the correction factor for controlling the degree of the user's trust reduction, which is a constant greater than 1.

Equation 4(d) represents the changing process of the user's trust value when the user's risk is lower than the risk threshold; q is a constant greater than 1, which is used to adjust the degree of the increased trust value.

It can be seen that the user's trust and risk values have the following relationship:

(a) The change in the user's trust value is negatively correlated to their risk value; the higher the risk value, the lower the trust value

(b) If the user's risk value is higher than the risk threshold, the user's trust value will decline at an increasing rate when the risk value increases

(c) When the risk value is higher than the risk threshold, the reduction of the risk value will not lead to an increase of trust; only after the risk value is below the risk threshold will a decrease in risk value lead to a rebound of the trust value

(d) The establishment of the user's trust value is a slow process that requires a long time

(e) We can control the user's access authority according to their risk and trust values

3.6. Authority Control. In order to provide a reliable process of risk assessment and authorization, as well as to storing a user's access right safely, a blockchain, as a trusted third-party database, is used in our scheme. The smart contract updates the user's access right based on his risk value and trust value. The information of the user can be queried through the interface provided by the blockchain. In addition, the user's real name will be replaced by a pseudonym to protect privacy and anonymity.

The smart contract in the Hyperledger Fabric is called chaincode. It can be used to implement transactions on the Fabric. Docker (Docker Inc., US) is used as a sandbox. After the chaincode is written according to the predetermined scene, it will be installed and instantiated on the blockchain. The deployed contract is packaged into a Docker image; each node launches a new Docker container. The codes execute the instantiation method in the contract, waiting for use.

In our scheme, the user's access is controlled by a smart contract deployed on the blockchain. The process of its implementation is as follows. First, the user's risk value and trust value, which are derived in the risk assessment step, are sent to the smart contract. Second, the smart contract updates the user access rights based on these values to prepare for the next authentication. When the system receives an access request by a user the next time, if the password authentication passes, the chaincode will be executed, and a query is issued through the smart contract interface provided by the Fabric. Finally, the user's access right will be returned. Owing to the application of the blockchain, the user's access right has become safer and more credible.

4. Results and Discussion

In this section, we will analyze the security and performance of our scheme. First, we will use SVO logic (Syverson–van Oorschot) to verify the third step, which takes charge of the authentication of the user's identity. We will then discuss other features of our program.

4.1. Certification Based on SVO Logic

4.1.1. SVO Logic. SVO logic is an extension of BAN logic (Burrows–Abadi–Needham) [51]. It is based on the summary of logical systems such as BAN logic [52], GNY logic (Gong–Needham–Yahalom) [53], AT logic [54], and VO logic [55]. The appearance of SVO logic indicates the maturity of BAN logic. It not only has the advantages of BAN logic but is also very simple and easy to use. SVO logic provides us with a detailed model that greatly eliminates the confusion of the meaning and inference rules of logical expressions. By using the formal description based on SVO logic, we can accurately understand the true meaning of the protocol. This is the main reason why SVO logic is used to demonstrate the authentication phase in our scheme.

The following are the basic axioms involved in analyzing security in this study:

Source Association axioms:

Rule 1: $(P \overset{K}{\leftrightarrow} Q \wedge R \triangleleft \{X^Q\}_K)^{(Q|\sim X \wedge Q \ni K)}$

Saying axioms:

Rule 2: $P| \approx (X_1, \ldots, X_n)^{(P|\sim (X_1,\ldots,X_n) \wedge P| \approx X_i)}$

Jurisdiction axioms:

Rule 3: $(P| \Rightarrow \varphi \wedge P| \approx \varphi)^{\varphi}$

Freshness axioms:

Rule 4: $\#(X_i)^{\#(X_1,\ldots,X_n)}$

Nonce-verification axioms:

Rule 5: $(\#(X) \wedge P| \sim X)^{P| \approx X}$

Symmetric goodness of shared keys axioms:

Rule 6: $P \overset{K}{\leftrightarrow} Q \equiv Q \overset{K}{\leftrightarrow} P$

4.1.2. Security Analysis. Next, the third step is modeled. The following notation is used: U stands for the user; S stands for the server; Tu and Ts stand for the timestamp; k stands for the cryptographic key between U and S. For the information entered by the user, we describe it as (IDu, PWu). For the final result of the password authentication and permission value, we record it as Ns. Then, we get the following process:

Message 1: $U \longrightarrow S$: $\{(\mathrm{IDu}, \mathrm{PWu}), \#(\mathrm{Tu})\}k$

Message 2: $S \longrightarrow U$: $\{(\mathrm{Ns}), \#\mathrm{Ts}\}k$

The goal of the authentication phase is to be confident that the user will receive a credible authentication result. The necessary condition is that one believes the other can control the message, which is generated by itself, and they all believe

that everyone has the correct cryptographic key to ensure the security of the whole communication. Based on this, we describe the objectives and initial assumptions as follows:

Goal: $U| \equiv \mathrm{Ns}$

Initial state assumptions:

A1: $U| \equiv U \overset{k}{\leftrightarrow} S$
A2: $S| \equiv S \overset{k}{\leftrightarrow} U$
A3: $S| \equiv \#(\mathrm{Tu})$
A4: $U| \equiv \#(\mathrm{Ts})$
A5: $U| \equiv S \Rightarrow \mathrm{Ns}$
A6: $S| \equiv U \Rightarrow (\mathrm{IDu}, \mathrm{PWu})$

According to the initial state assumptions, the SVO logic system is used to verify the security of the authentication process.

From A2, we apply the symmetric goodness of shared keys axioms to obtain the following.

Step 1. $S| \equiv U \overset{k}{\leftrightarrow} S$, $S| \equiv S \overset{k}{\leftrightarrow} U$

From message 1, step 1, we apply the source association axioms to obtain the following.

Step 2. $S| \equiv U| \sim ((\mathrm{IDu}, \mathrm{PWu}), \#(\mathrm{Tu}))$

From A3, we apply freshness axioms to obtain the following.

Step 3. $S| \equiv \#((\mathrm{IDu}, \mathrm{PWu}), \mathrm{Tu})$

From Step 2 and Step 3, we apply nonce-verification axioms to obtain the following.

Step 4. $S| \equiv U| \approx ((\mathrm{IDu}, \mathrm{PWu}), \mathrm{Tu})$

From A6 and Step 4, we apply saying axioms and jurisdiction axioms to obtain the following.

Step 5. $S| \equiv (\mathrm{IDu}, \mathrm{PWu})$

It can be seen that if S correctly received the message sent by the user, then it can authenticate the user based on the message.

From A1, we apply symmetric goodness of shared keys axioms to obtain the following.

Step 6. $U| \equiv U \overset{k}{\leftrightarrow} S$, $U| \equiv S \overset{k}{\leftrightarrow} U$

From message 2, Step 6, we apply source association axioms to obtain the following.

Step 7. $U| \equiv S| \sim (\mathrm{Ns}, \#(\mathrm{Ts}))$

From A4, we apply freshness axioms to obtain the following.

Step 8. $U| \equiv \#(\mathrm{Ns}, \mathrm{Ts})$

From Steps 7 and 8, we apply nonce-verification axioms to obtain the following.

Step 9. $U| \equiv S| \approx (\mathrm{Ns}, \mathrm{Ts})$

From A5, Step 9, we apply saying axioms and jurisdiction axioms to obtain the following.

Step 10. $U| \equiv \mathrm{Ns}$

Up to now, the initial goal has been proved. From the above SVO logic analysis, we can achieve the security authentication between the user and the server, and other processes can also be secured in a similar manner.

4.2. Other Performance Analyses. In addition to inheriting the advantages of traditional password authentication, our solution also has the following characteristics.

4.2.1. Resist Replay Attack. Replay attack [56] means that the attacker sends a packet that has been received by the target host in order to spoof the system. It mainly occurs in the identity authentication process, affecting the correctness of the authentication.

Threat situation assumption: consider the following two attack situations during the user registration and authentication phase.

Situation 1: as shown in Figure 2, in the authentication phase, the user U sends an access request message $\{T, ID, psw'\}\ k$ to the server S. Attacker A intercepts and resends the message $\{T*, ID, psw'\}\ k$, where $T*$ is the timestamp of this repeated sent message.

Situation 2: as shown in Figure 3, in the registration phase, the user U sends a registration request message $\{T, ID, psw'\}\ k$ to the server S. Assuming U is held by the attacker, U will resend the message $\{T*, ID, psw'\}\ k$, where $T*$ is the timestamp of the second sent message.

In our scheme, the timestamp T can be used if the timestamp is mismatched at the user's end due to an incomplete or corrupted request, which can ensure that the correct requests are received from the client. It also can be used in resisting replay attacks. ΔT is the maximum transfer delay. If $|T - T^*| > \Delta T$, then S will discard the message. Similarly, when the user receives the identity authentication result, the timestamp will be used. If the attacker resends the message, the timestamp verification will fail, and the user will discard the message. Therefore, the proposed solution can resist replay attacks.

4.2.2. Greater Flexibility and Security. The user's authority is no longer static; his authority changes with his risky behavior. The user's authority determines whether he can pass the identity authentication. Thus, the user's identity authentication has continuity and mutability.

We choose the authentication step in our scheme because it is the most frequent and important one. In this step, we consider the following three attack situations.

Situation 1: attacker A attempts to steal the account of user U by guessing his password. Each failed attempt by attacker A will be recorded as a risk behavior of the account. After a while, even if attacker A successfully guesses the username and password, he may lose access due to excessive risk.

Situation 2: attacker A steals a user's password to log in. Because the attacker's IP address and MAC address are different from those of the real user, these differences will be recorded as being risky. The stolen account's risk will

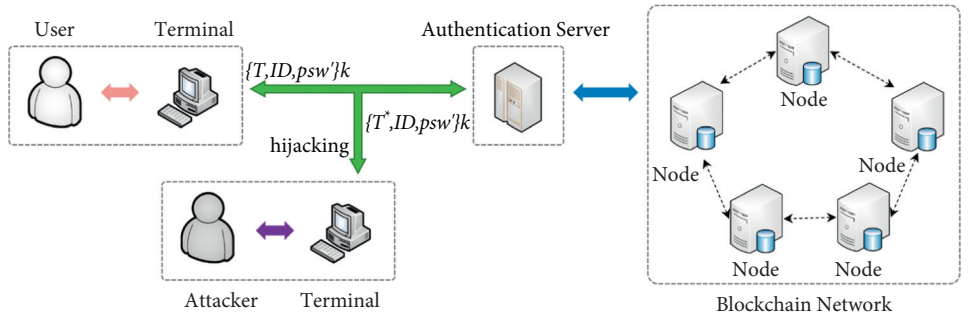

Figure 2: Replay attack scenario 1.

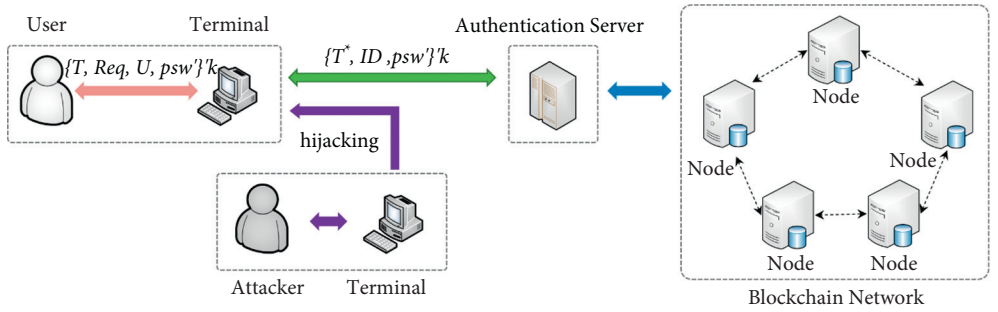

Figure 3: Replay attack scenario 2.

increase and his trust value will decrease. As a result, the attacker may lose his access right.

Situation 3: attacker A holds the account of user U to perform high-risk operations, such as modifying the login password and sensitive information or executing some unauthorized operations. This risky behavior will be recorded and the risk value of the user will increase rapidly. Thus, the user will lose his account right.

It can be seen that compared with the traditional password authentication method, our scheme combines dynamic authority control with traditional static identity authentication. Even if the user passes the password authentication, the user is not considered reliable; they must have enough access rights.

4.2.3. Mutual Authentication. The methods presented in the *Certification based on the SVO logic* section prove that in our scheme, user U and server S can trust each other. Therefore, our program has achieved mutual authentication.

4.2.4. Security of User's Risk Assessment and Access Control. Smart contracts allow trusted execution without third parties, and the contract content is transparent and irreversible. Using a smart contract to manage the user's risk and authority can guarantee the security of the generation process of the access right. In addition, in order to ensure the anonymity of a user on the blockchain, we write the user's pseudonym into the blockchain.

4.2.5. Efficiency and Performance. We mainly consider the calculation time of the authentication phase because this phase is the central part of our method and is executed more frequently than other steps. We next consider the scenario of the process of user access to campus networks. Considering the small size of our network, we choose 1, 10, 50, and 100 users, and test 100 times in the scenario when these users access simultaneously.

The network server consists of the following:

Processor: Intel® Core™ i5-4200M CPU @ 2.50 GHz

RAM: 6.00 GB

Bandwidth: 100 Mbps

We have analyzed the comparison results in Figure 4. The subgraph 4(a) shows the average access latency of the users. As can be seen from the figure, our scheme has strong stability. The subgraph 4(b) shows the mean and variance of the experiment, which is different for concurrent visits and reflects the changing trend of response time required from individual users. It can be seen that even for the case of initiating a concurrent login by multiple users, the impact on the efficiency of our solution is still acceptable. At the same time, since the focus of our plan is to ensure the users' access security, correspondingly, our solution will sacrifice some performance. However, we still optimize the efficiency of the program. There are not very many operations for the server to execute in the authentication process. When requesting access, we need not perform excessive and complicated operations such as encryption and decryption to realize the conversion of the user's name and pseudonym, but only to verify the correctness of the equation to ensure the consistency of the name and the pseudonym. While overcoming some security deficiencies, this also improves efficiency.

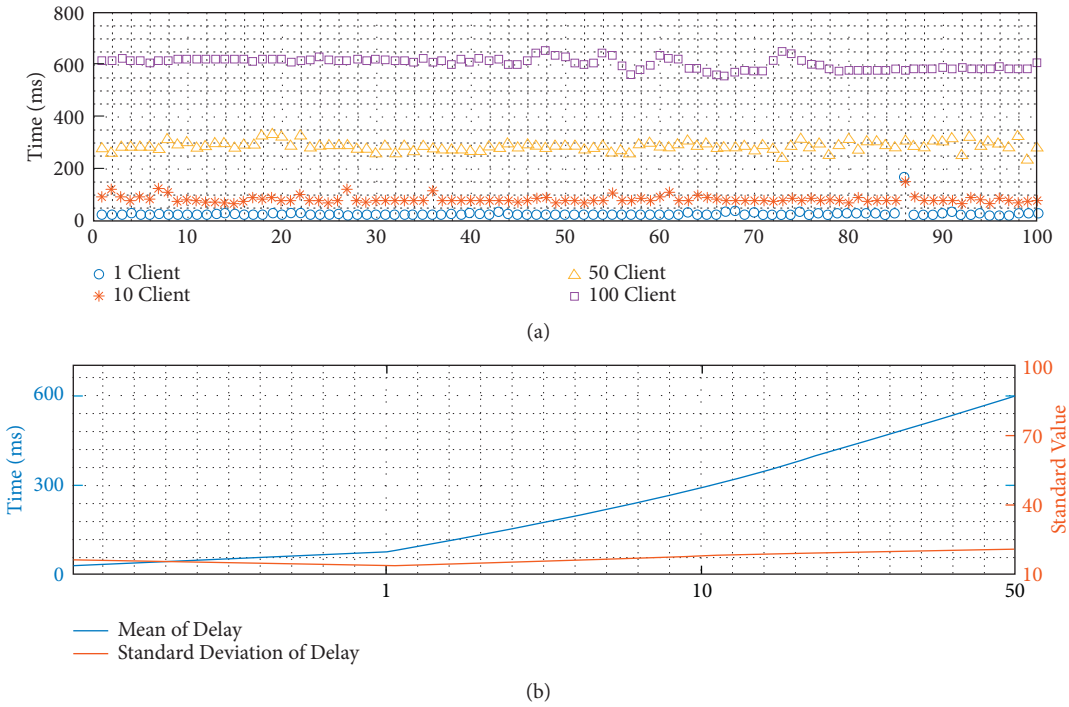

Figure 4: User's access time. (a) Access delay; (b) delay trend.

4.2.6. Scalability. Our scheme has good expansibility, mainly in the following manners:

(a) The password authentication method used in this study can be replaced by other authentication methods. According to the security and convenience requirements of different scenarios, more complex or more efficient authentication can be used.

(b) The method of risk grading can be developed with flexibility. For the requirements of different scenarios, the risk behavior can be divided into different levels. For example, company and university networks may have different risk behaviors, and the corresponding grading strategy can be developed accordingly.

(c) With the development of blockchain technology, the blockchain platform used in our scheme can be replaced by others. Administrators can choose another blockchain platform to optimize the scheme.

5. Conclusions

In the complex and variable network environment, higher demands are presented for the continuity and mutability of identity authentication. The UCON model can achieve the requirements of the current network to some extent, but it still has some weaknesses. Based on this, we proposed a risk-based dynamic identity authentication method based on the UCON model, combining risk assessment and authority control with password authentication. Blockchain technology is used to provide reliable processes for risk assessment and authorization.

We described our identity authentication scheme in detail. The scheme includes initialization, registration, authentication, user resource access, risk assessment, and authority control. In the authentication step, we combined password authentication and access control results to determine whether the user can pass the authentication. In the step of risk assessment, we evaluated the user's historical risk behavior and derived their risk value and trust value. In the authority control step, we uploaded the user's related information on the blockchain and controlled the user's access rights with smart contracts.

In this study, we analyzed the security of our authentication scheme. We used SVO logic to describe the access step of the plan, using inference rules and axioms to prove that our scheme is safe and feasible. Subsequently, we analyzed our scheme in a variety of attack scenarios, showing that our solution can withstand attacks in multiple network environments. Finally, we simulated the university's network environment to test our scheme. The experimental results show that our solution has good stability and can guarantee login efficiency.

Our scheme represents an improvement of traditional identity authentication, having higher continuity and mutability. It has also been proved that the scheme has high security and efficiency. In addition, our scheme is highly scalable and can be applied to a variety of scenarios where users require authentication.

Data Availability

The paper used the inference rules and axioms of the SVO logic system to formally verify the protocol. Further, it used back-end analysis modules such as OFMC and CL-AtSe of the AVISPA tool to test the protocol logic. No data were used to support this study.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was partly supported by the National Key Research and Development Project (Key Technologies and Applications of Security and Trusted Industrial Control System no. 2020YFB2009500), Beijing Municipal Natural Science Foundation (19L2020), the Industrial Internet Innovation and Development Project (Typical application and promotion project of the security technology for the electronics industry) of the Ministry of Industry and Information Technology of China in 2018, and the Foundation of Shaanxi Key Laboratory of Network and System Security (grant no. NSSOF1900105).

References

[1] Internet World Stats, "Internet usage statistics; "The Internet big picture: world Internet users and 2019 population stats"," 2019, https://www.internetworldstats.com/stats.htm. Internetworldstats 2019.

[2] M. B. Mollah, M. A. K. Azad, and A. Vasilakos, "Secure data sharing and searching at the edge of cloud-assisted internet of things," *IEEE Cloud Computing*, vol. 4, no. 1, pp. 34–42, 2017.

[3] S. Widup, M. Spitler, D. Hylender, and G. Bassett, "Verizon data breach investigations report," Technical Report, 2018.

[4] A. Mirian, J. DeBlasio, S. Savage, G. M. Voelker, and K. Thomas, "Hack for hire: exploring the emerging market for account hijacking," 2019, https://www.sysnet.ucsd.edu/~voelker/pubs/hackforhire-www19.pdf.

[5] Akamai Technologies, "Soti-2018-credential-stuffing-attacks-report," 2019, https://www.akamai.com/cn/zh/multimedia/documents/state-of-the-internet/soti-2018-credential-stuffing-attacks-report.pdf.

[6] Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for Internet of Things," *Journal of Network and Computer Applications*, vol. 42, pp. 120–134, 2014.

[7] Y. A. Qadri, A. Nauman, Y. B. Zikria, A. V. Vasilakos, and S. W. Kim, "The future of healthcare Internet of Things: a survey of emerging technologies," *IEEE Communications Surveys & Tutorials*, vol. 22, 2020.

[8] J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos, "Security and privacy for cloud-based IoT: challenges," *IEEE Communications Magazine*, vol. 55, no. 1, pp. 26–33, 2017.

[9] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the internet of things: perspectives and challenges," *Wireless Networks*, vol. 20, no. 8, pp. 2481–2501, 2014.

[10] A. Lazouski, G. Mancini, F. Martinelli, and P. Mori, "Usage control in cloud systems," in *Proceedings of the International Conference for Internet Technology and Secured Transactions (ICITST)*, pp. 202–207, IEEE, London, UK, December 2013.

[11] The Internet Engineering Task Force, "Internet security glossary," 2019, https://datatracker.ietf.org/doc/rfc2828.

[12] A. Ouda, "A framework for next generation user authentication," in *Proceedings of the 2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC)*, pp. 1–4, IEEE, Muscat, Oman, March 2016.

[13] F. Y. Yang, C. W. Hsu, and S. H. Chiu, "Password authentication scheme preserving identity privacy," in *Proceedings of the 2014 Sixth International Conference on Measuring Technology and Mechatronics Automation*, pp. 443–447, IEEE, Zhangjiajie, China, January 2014.

[14] R. Song, "Advanced smart card based password authentication protocol," *Computer Standards & Interfaces*, vol. 32, no. 5-6, pp. 321–325, 2010.

[15] S. Jangirala, S. Mukhopadhyay, and A. K. Das, "A multi-server environment with secure and efficient remote user authentication scheme based on dynamic ID using smart cards," *Wireless Personal Communications*, vol. 95, no. 3, pp. 2735–2767, 2017.

[16] V. Odelu, A. K. Das, and A. Goswami, "A secure biometrics-based multiserver authentication protocol using smart cards," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 9, pp. 1953–1966, 2015.

[17] D. He and D. Wang, "Robust biometrics-based authentication scheme for multiserver environment," *IEEE Systems Journal*, vol. 9, no. 3, pp. 816–823, 2015.

[18] J. Sun, Q. Zhong, L. Kou, W. Wang, Q. Da, and Y. Lin, "A lightweight multifactor mobile user authentication scheme," in *Proceedings of the IEEE INFOCOM 2018 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pp. 831–836, IEEE, Honolulu, HI, USA, April 2018.

[19] S. Challa, A. K. Das, V. Odelu et al., "An efficient ECC-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks," *Computers & Electrical Engineering*, vol. 69, pp. 534–554, 2018.

[20] Z. Yan, P. Zhang, and A. V. Vasilakos, "A security and trust framework for virtualized networks and software-defined networking," *Security and Communication Networks*, vol. 9, no. 16, pp. 3059–3069, 2016.

[21] M. Wazid, A. K. Das, V. Vivekananda Bhat, and A. V. Vasilakos, "LAM-CIoT: lightweight authentication mechanism in cloud-based IoT environment," *Journal of Network and Computer Applications*, vol. 150, 2020.

[22] H. Vasudev, D. Das, and A. V. Vasilakos, "Secure message propagation protocols for IoVs communication components," *Computers & Electrical Engineering*, vol. 82, Article ID 106555, 2020.

[23] Y. Lai, Y. Chen, Q. Zou, Z. Liu, and Z. Yang, "Design and analysis on trusted network equipment access authentication protocol," *Simulation Modelling Practice and Theory*, vol. 51, pp. 157–169, 2015.

[24] P. Porambage, M. Ylianttila, C. Schmitt, P. Kumar, A. Gurtov, and A. V. Vasilakos, "The quest for privacy in the internet of things," *IEEE Cloud Computing*, vol. 3, no. 2, pp. 36–45, 2016.

[25] RSA Security, "RSA risk-based authentication," 2019, http://webobjects.cdw.com/webobjects/media/pdf/rsa/H11465_RBA_WP_0113.pdf?cm_sp=RSAShowcase-_-Cat1Link4-_SecurID+White+Paper.

[26] B. Luo and Y. Liu, "The risk evaluation model of network information security based on improved BP neural network,"

vol. 1, pp. 189–191, in *Proceedings of the 2012 International Symposium on Instrumentation & Measurement, Sensor Network and Automation (IMSNA)*, vol. 1, IEEE, Sanya, China, August 2012.

[27] P. Patil, P. Zavarsky, D. Lindskog, and R. Ruhl, "Fault tree analysis of accidental insider security events," in *Proceedings of the 2012 International Conference on Cyber Security*, pp. 113–118, IEEE, Alexandria, VA, USA, 14 December 2012.

[28] Q. Hong, T. Jianwei, T. Zheng et al., "An information security risk assessment method based on conduct effect and dynamic threat," in *Proceedings of the 2017 8th IEEE International Conference on Software Engineering and Service Science (ICSESS)*, pp. 782–786, IEEE, Beijing, China, November 2017.

[29] M. Wazid, A. K. Das, N. Kumar, A. V. Vasilakos, and J. J. P. C. Rodrigues, "Design and analysis of secure lightweight remote user authentication and key agreement scheme in Internet of Drones deployment," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3572–3584, 2019.

[30] M. Wazid, A. K. Das, N. Kumar, M. Conti, and A. V. Vasilakos, "A novel authentication and key agreement scheme for implantable medical devices deployment," *IEEE Journal of Biomedical and Health Informatics*, vol. 22, no. 4, pp. 1299–1309, 2018.

[31] S. Challa, A. K. Das, P. Gope, N. Kumar, F. Wu, and A. V. Vasilakos, "Design and analysis of authenticated key agreement scheme in cloud-assisted cyber-physical systems," *Future Generation Computer Systems*, vol. 108, pp. 1267–1286, 2020.

[32] A. Kosba, A. Miller, E. Shi, Z. Wen, and P. C. Hawk, "The blockchain model of cryptography and privacy-preserving smart contracts," in *Proceedings of the 2016 IEEE Symposium on Security and Privacy (SP)*, pp. 839–858, IEEE, San Jose, CA, USA, 22 May 2016.

[33] K. Fan, Z. Bao, M. Liu, A. V. Vasilakos, and W. Shi, "Dredas: decentralized, reliable and efficient remote outsourced data auditing scheme with blockchain smart contract for industrial IoT," *Future Generation Computer Systems*, vol. 11, 2020.

[34] C. Lin, D. He, X. Huang, K.-K. R. Choo, and A. V. Vasilakos, "BSeIn: a blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0," *Journal of Network and Computer Applications*, vol. 116, pp. 42–52, 2018.

[35] T. Sanda and H. Inaba, "Proposal of new authentication method in Wi-Fi access using Bitcoin 2.0," in *Proceedings of the 2016 IEEE 5th Global Conference on Consumer Electronics*, pp. 1–5, IEEE, Kyoto, Japan, October 2016.

[36] S. Jangirala, A. K. Das, and A. V. Vasilakos, "Designing secure lightweight blockchain-enabled RFID-based authentication protocol for supply chains in 5G mobile edge computing environment," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 11, pp. 7081–7093, 2020.

[37] S. Raju, S. Boddepalli, S. Gampa, Q. Yan, and J. S. Deogun, "Identity management using blockchain for cognitive cellular networks," in *Proceedings of the 2017 IEEE International Conference on Communications (ICC)*, pp. 1–6, IEEE, Paris, France, May 2017.

[38] 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.

[39] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: the case study of a smart home," in *Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pp. 618–623, IEEE, Kona, HI, USA, March 2017.

[40] G. Zyskind and O. Nathan, "Decentralizing privacy: using blockchain to protect personal data," in *Proceedings of the 2015 IEEE Security and Privacy Workshops*, pp. 180–184, IEEE, San Jose, CA, USA, May 2015.

[41] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[42] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "Medrec: using blockchain for medical data access and permission management," in *Proceedings of the 2016 2nd International Conference on Open and Big Data (OBD)*, pp. 25–30, IEEE, Vienna, Austria, August 2016.

[43] A. Ramachandran and D. Kantarcioglu, "Using blockchain and smart contracts for secure data provenance management," 2017, https://arxiv.org/abs/1709.10000.

[44] Y. Liu, K. Wang, Y. Lin, and W. Xu, "LightChain: a lightweight blockchain system for industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3571–3581, 2019.

[45] C. Qiu, F. R. Yu, H. Yao, C. Jiang, F. Xu, and C. Zhao, "Blockchain-based software-defined industrial Internet of Things: a dueling deep Q-learning approach," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4627–4639, 2019.

[46] Wikipedia, "One-key_MAC," 2019, https://en.wikipedia.org/wiki/One-key_MAC.

[47] J. C. Choon and J. H. Cheon, *An Identity-Based Signature from gap Diffie-Hellman Groups*, Springer, Berlin, Heidelberg, Germany, 2003.

[48] G. Neelima and S. Rodda, "Predicting user behavior through sessions using the web log mining," in *Proceedings of the 2016 International Conference on Advances in Human Machine Interaction (HMI)*, pp. 1–5, IEEE, Kodigehalli, India, March 2016.

[49] V. Visintine, *An Introduction to Information Risk Assessment*, SANS Institute, Bon-y-maen, UK, 2003.

[50] General Administration of Quality Supervision, "Inspection and quarantine of people's Republic of China. GB/T 20984-2007," *Information Security Technology: Risk Assessment Specification for Information Security*, GB/T 20984-2007, China, 2007.

[51] L. Chen and M. Shi, "Security analysis and improvement of Yahalom protocol," in *Proceedings of the 2008 3rd IEEE Conference on Industrial Electronics and Applications*, pp. 1137–1140, IEEE, Singapore, June 2008.

[52] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," *ACM SIGOPS-Operating Systems Review*, vol. 23, no. 5, pp. 1–13, 1989.

[53] L. Gong, R. Needham, and R. Yahalom, "Reasoning about belief in cryptographic protocols," in *Proceedings of the 1990 IEEE Computer Society Symposium on Research in Security and Privacy*, pp. 234–248, IEEE, Oakland, CA, USA, May 1990.

[54] M. N. Abadi and M. R. Tuttle, "A semantics for a logic of authentication," in *Proceedings of the Tenth Annual ACM Symposium on Principles of Distributed Computing*, vol. 8, no. 1, pp. 18–36, ACM, Montreal Quebec Canada, August 1991.

[55] P. V. Oorschot, "Extending cryptographic logics of belief to key agreement protocols," in *Proceedings of the 1st ACM Conference on Computer and Communications Security*, pp. 232–243, ACM, Fairfax Virginia USA, November 1993.

[56] P. Rughoobur and L. Nagowah, "A lightweight replay attack detection framework for battery depended IoT devices designed for healthcare," in *Proceedings of the 2017*

International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions) (ICTUS), pp. 811–817, IEEE, Dubai, United Arab Emirates, December 2017.