Hindawi
Mobile Information Systems
Volume 2023, Article ID 4764135, 13 pages
https://doi.org/10.1155/2023/4764135

Research Article

Blockchain-Based Authentication Scheme with an Adaptive Multi-Factor Authentication Strategy

Yanbin Xu,[1] **Xinya Jian**,[2] **Tao Li**,[2] **Shuang Zou**,[3] **and Beibei Li**[2]

[1]*College of Computer Science, Sichuan University, Chengdu 610065, China*
[2]*School of Cyber Science and Engineering, Sichuan University, Chengdu 610065, China*
[3]*Sichuan Public Project Consulting Management Co., Chengdu 610041, China*

Correspondence should be addressed to Beibei Li; libeibei@scu.edu.cn

Received 5 January 2023; Revised 3 June 2023; Accepted 14 June 2023; Published 14 November 2023

Academic Editor: Peiying Zhang

Authentication is of paramount significance to cybersecurity. However, most of conventional authentication schemes are implemented in a centralized mode, in which potential problems that could arise include single-point failure, the exposure of personal information, and the risk of identity theft. Additionally, static single-factor authentication schemes are unsuitable for dynamic environments like mobile applications. In order to tackle these difficulties, we propose a blockchain-based authentication scheme with an adaptive multi-factor authentication strategy. Our scheme features a blockchain-based authentication framework that prevents unauthorized information alteration and system corruption. Additionally, we design an adaptive multi-factor authentication strategy model to ensure trustworthy multi-factor authentication in dynamic scenarios. Last, we construct a Raft-based consensus model to select an authoritative leading node for rapid authentication. The security analysis demonstrates the effectiveness of the proposed scheme in effectively countering various forms of cyberattacks targeted at authentication systems, and experiments demonstrate its superior effectiveness and efficiency compared to existing studies.

1. Introduction

In recent times, due to the rapid advancement and extensive adoption of Internet technology, the number of large-scale distributed mobile systems has increased, necessitating trust and security services to reduce the risk of illegal access. Authentication schemes are crucial for ensuring mobile network security and privacy by providing data confidentiality, audit confirmation, and authorization control. As shown in Figure 1, a typical authentication process involves storing private identification information in a centralized mobile server, making them vulnerable to attack methods that can compromise user identity information or disrupt authentication services. Additionally, centralized authentication architectures are unreliable in providing adequate protection for computing devices and applications. From the perspective of service providers, managing and verifying users will inevitably become complex and vulnerable to many mobile network security risks, including but not limited to the following: the occurrence of single-point failure, privacy breaches, and the risk of identity theft [1]. Centralized storage of personal identity information on servers creates a potential target for malicious attacks that can compromise the authentication service and lead to the corruption or theft of user authentication information. For instance, in 2014, attackers stole approximately 200 photographs of female Hollywood entertainers, including private and nude content, and uploaded them to social media sites [2]. The investigation revealed that attackers had cracked usernames and passwords stored centrally on servers and used the information to log into mobile applications as legitimate users.

As the vulnerabilities of centralized authentication architectures have become increasingly evident, there is a growing interest in developing decentralized authentication solutions. One potential solution is to leverage blockchain technology, a decentralized, secure, and trustworthy architecture that is capable of preserving time-series data [3].

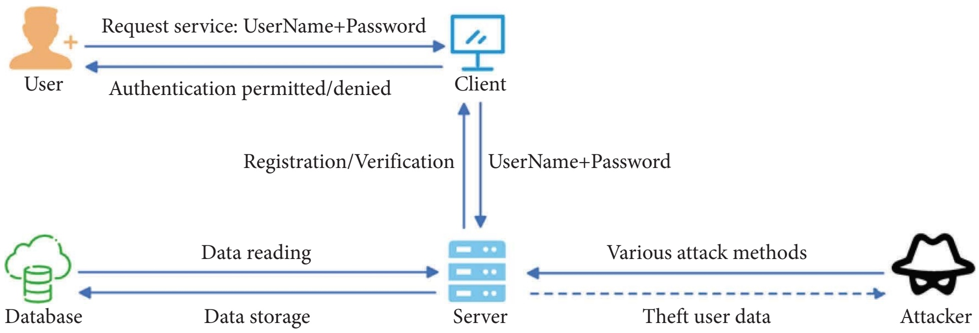

Figure 1: The conventional authentication process.

Blockchain technology utilizes a decentralized, peer-to-peer mobile network structure, enabling services to remain available even if some nodes fail. The process of verifying, accounting, and broadcasting blockchain data uses a time-stamped chain block structure that provides extreme verifiability and traceability, adding a temporal dimension to the data. Within the blockchain system, a particular consensus mechanism is utilized to guarantee the uniformity among all nodes. This mechanism enables the timely detection of malicious nodes, defends against external attacks, and prevents blockchain data from being tampered with or falsified [4]. The consensus mechanism plays a vital role in ensuring the security and reliability of the blockchain. It safeguards against malicious nodes attempting to manipulate the blockchain by enforcing a requirement for majority agreement among network nodes before any modifications to the blockchain can take place. Additionally, the consensus mechanism provides a mechanism for the network to recover from failures or attacks by ensuring that a consistent state is maintained across all nodes in the network. These characteristics of decentralization, security, and traceability make blockchain technology a promising solution for developing authentication systems. Indeed, researchers have recently begun to explore the potential of combining blockchain technology and authentication schemes to enhance mobile network security [5–11]. It is noteworthy that due to the high degree of privacy associated with identity authentication information, it is imperative to ensure the privacy and security of identity authentication information which is crucial, particularly in a decentralized storage structure, due to the sensitive nature of this data. Therefore, users should only disclose their private information to a select few trusted institutions [12, 13].

Authentication factors, including biological, physical factors, and password factors, are essential for verifying user identity. Due to the recent security threats, authentication schemes based on static and single factors are no longer reliable to adequately protect authentication devices and applications. To ensure ongoing safeguarding of computing devices and essential mobile services against unauthorized access, security can be enhanced by combining authentication techniques from different factors. This approach, commonly referred to as multi-factor authentication (MFA), utilizes a combination of factors to strengthen security [14]. MFA is becoming increasingly necessary due to the growing sophistication and frequency of cyberattacks, which can compromise user credentials and lead to unauthorized access. MFA can enhance security by requiring multiple forms of authentication, making it more challenging for attackers to bypass or compromise authentication. One of the key challenges in implementing MFA is determining the optimal set of authentication factors to use in a given operating environment. This challenge arises because there are many possible factors that can be used for authentication, each with its own strengths and weaknesses, and no one solution can address all authentication requirements [15]. The effectiveness of MFA heavily relies on choosing the right combination of authentication factors. Using too few factors will leave systems vulnerable to attacks while using too many will create a cumbersome and time-consuming authentication process that may deter users from adopting MFA. Moreover, the selection of the wrong factors or the incorrect number of factors can increase the risk of data breaches, since attackers may be able to bypass the authentication process. To address this challenge, organizations need to carefully evaluate the risks and requirements of their operating environment and select the most appropriate authentication factors accordingly. The appropriateness of biometric data, passwords, tokens, and mobile devices as authentication factors may vary depending on the use case, and the combination of factors should be customized to suit the requirements of each organization. Adopting adaptive MFA presents a potential solution to address this challenge. This approach allows for the dynamic adjustment of authentication factors based on the operating environment and the associated risk level. This approach can ensure that only the most trustworthy and relevant factors are used to validate users, providing an additional layer of security and flexibility for organizations.

Motivated by the aforementioned discussion, this paper introduces a novel authentication scheme that leverages blockchain technology and incorporates an adaptive multi-factor authentication approach. Our work contributes in three main aspects, outlined below:

(1) First, a secure and decentralized authentication framework is proposed to prevent unauthorized access and data tampering.

(2) Second, an adaptive multi-factor authentication (A-MFA) strategy model is developed to select the most

trustworthy multi-factor set for authentication in dynamic scenarios, such as mobile applications.

(3) Last, a consensus model, named Limited-Raft (LRaft), is designed based on the Raft algorithm to vote for an authoritative leading node to conduct rapid and secure authentication over the blockchain.

The rest of this article is structured as follows. Section 2 provides a review of recent studies on blockchain-based identity authentication schemes. Section 3 presents the system model and threat model considered in this study. Section 4 details the proposed blockchain-based scheme. Section 5 presents the performance evaluation. Finally, Section 6 concludes the article.

2. Related Work

In this section, we present a concise overview of the latest advancements in authentication schemes that incorporate blockchain and multi-factor authentication. These studies are important in advancing the field of information security as they provide new insights and solutions that can enhance the security and reliability of authentication systems, protecting computing devices and critical mobile services from malicious attacks and unauthorized access.

2.1. Blockchain-Based Authentication Scheme. Blockchain-based identity authentication frameworks have sparked a boom in scholarly research in recent years due to their decentralized, secure, and trustworthy architecture. Researchers have proposed a range of authentication schemes that incorporate blockchain technology, including methods for secure data transmission and authentication protocols that can resist various types of cyberattacks. In 2019, Jangirala et al. [5] proposed a blockchain-based RFID authentication protocol specifically tailored for the supply chain of 5G mobile edge computing. This protocol aimed to enhance efficiency and security in the authentication process. It used Internet security protocols and automatic application verification for security verification and could protect against various attacks. In 2020, Guo et al. [7] proposed a distributed authentication system that combines blockchain and edge computing, improving authentication efficiency. The system includes a blockchain edge layer, a blockchain network layer, and an optimized Byzantine fault-tolerant consensus algorithm for creating a consortium chain to store authentication data and logs. In 2021, Zhang et al. [8] developed a hierarchical multi-access edge computing framework based on blockchain for the future VANET ecosystem. They introduced a multi-factor trust model within the VANET environment to assess the trustworthiness of vehicles through offloading calculations. This approach ensures the security of communication links between vehicles. In 2022, Xu et al. [9] proposed a blockchain-based cross-domain biometric authentication scheme that tackles the problem of biometric leakage by utilizing fuzzy extraction technology to extract random biometric authentication keys. In the same year, Zhang et al. [10] developed a blockchain-based multi-factor authentication protocol for privacy protection and cross-domain IoT, utilizing hardware fingerprints to generate random numbers encoded with multiple factors and transforming them into computational data. The blockchain stores dynamic accumulators for each domain, reducing overhead, and on-chain accumulators are employed to verify the identity of cross-domain industrial IoT devices. In 2023, Wang et al. [11] proposed a blockchain-based access control framework which includes an automated quality control mechanism and an authentication mechanism to guarantee the quality of training data and filter out malicious attackers. Simulated experiments validate the effectiveness of the proposed framework in ensuring the security of genetic data while maintaining a balance between availability and accuracy.

The abovementioned authentication systems combined with blockchain technology are primarily used for identification between specific IoT devices. However, there have been limited studies on general blockchain-based identification schemes.

2.2. Multi-Factor Authentication Scheme. MFA is another area of active research as it provides an extra layer of security by requiring two or more independent factors to verify a user's identity. Recent studies have investigated the effectiveness of MFA in various contexts, including mobile devices, cloud computing, and IoT systems. Researchers have proposed new methods for adaptive MFA, which can dynamically adjust the set of authentication factors based on the specific operating environment and level of risk involved. In 2016, Dasgupta et al. [16] developed a multi-factor selection framework for time-varying operating environments, considering factors such as equipment, media, and surrounding conditions, such as light, noise, motion, and more. User authentication is accomplished by employing a subset of authentication methods and their relevant features. In the same year, Wójtowicz and Joachimiak [17] developed a context-based biometric authentication model for mobile devices. Through a proof of concept, it determined the most accurate authentication method and the optimal form of validation interaction, laying the foundation for building adaptable and scalable multi-factor context-sensitive systems. In 2018, Roy and Dasgupta [18] used a probabilistic constrained nonlinear programming problem to evaluate the reliability of authentication methods in different user devices. Then, a fuzzy IF-THEN rule and genetic algorithm-based evolutionary strategy were developed for adaptively selecting authentication modes, which were validated through numerical simulation for their efficacy and efficiency. In 2021, Hassan et al. [19] proposed a multi-factor selection framework based on prior knowledge. By considering the context factors, the relevant requirements in the decision-making process, and the dynamic authentication method, the adaptive authentication system was developed. In 2022, Calvo and Beltrán [20] proposed a dynamic multi-factor selection model for heterogeneous, distributed, and dynamic environments, which can adjust security control strategies in real time to adapt to different risk scenarios. Based on a three-tier architecture and a three-step process including measure, decision, and adaption, the model can be adapted to different types of extensible policy and rule frameworks.

In summary, while MFA is an effective approach for enhancing security in authentication systems, it still faces challenges related to usability, implementation, and management cost. Addressing these challenges will require ongoing research and innovation in the field of information security to improve the effectiveness and usability of MFA solutions.

3. System Model and Threat Model

The present section provides an introduction to the system model and threat model adopted in this proposed scheme.

3.1. System Model. The system model comprises three entities, namely, the client, the authentication server, and the node server, as shown in Figure 2.

(1) *Client.* The client is responsible for collecting user authentication information through a factor collector, which is used to facilitate user-server interactions.

(2) *Authentication Server.* The authentication server operates an adaptive multi-factor authentication strategy model for the authentication process, handles authentication messages, and connects with the blockchain.

(3) *Node Server.* Multiple node servers are connected to form the blockchain. The authentication blockchain is a limited-access bulletin board. The entire authentication process is led by several trusted organizations, and blocks are generated through an LRaft consensus model designed to randomly select lead nodes in a rapid mode.

3.2. Threat Model. The threat model for a server-centric MFA scheme can be categorized into several categories, as follows:

(1) *Server Attacks.* The central server is vulnerable to various attacks, such as DDoS attacks, buffer overflow attacks, and SQL injection attacks. Once the server is compromised, the attackers can obtain access to all the user authentication information.

(2) *Single Point of Failure.* In this type of attack, if the central server fails, the authentication system would be completely down, and user authentication would be unavailable.

(3) *Unauthorized Access.* Attackers can bypass the MFA system by exploiting vulnerabilities in the system, such as by stealing user credentials or by intercepting SMS messages.

(4) *Insufficient Authentication Factor Selection.* MFA schemes should select an optimal set of authentication factors based on the operating environment. If an incorrect set of factors is selected, the system could become more vulnerable to attacks.

(5) *Social Engineering.* Attackers can use social engineering techniques to trick users into providing their authentication information. For example, attackers can impersonate IT support staff and ask users for their authentication information.

4. The Proposed Authentication Scheme

In this section, we provide a detailed description of the proposed scheme, beginning with an outline of the blockchain-based authentication framework, followed by an introduction to the A-MFA strategy model. Last, we introduce the LRaft consensus model.

4.1. Blockchain-Based Authentication Framework. Blockchain technology has received increasing attention in recent years due to its inherent properties such as decentralization, transparency, and security. In the realm of identity authentication, blockchain has emerged as a promising solution for improving the security and privacy of identity information. Traditional identity authentication systems have relied on centralized authorities to store and manage user information, which poses the risk of single points of failure and unauthorized access. Blockchain-based identity authentication frameworks offer a decentralized and tamper-resistant way of storing and managing identity data, thus enhancing security and privacy. The proposed scheme for identity authentication based on blockchain, as shown in Figure 3, is characterized by a robust structure that provides secure decentralized authentication services and ensures the prevention of unauthorized information alteration and system corruption. The authentication server connects to an A-MFA strategy model, which assists in selecting the appropriate factor group, while blockchain technology is employed to store identification information and record the authentication process. To ensure efficient and secure authentication, the content of the blockchain is maintained by a node cluster. The nodes in the cluster reach a consensus through the LRaft consensus model, which facilitates the generation of new blocks while ensuring rapid authentication.

To fulfill the requirements of identity verification, the block structure is designed as depicted in Figure 4. Each block comprises two main components: the block header and the block body. The block header includes essential attributes, such as the Index, PreHash, UserID, TimeStamp, and SignInfo. On the other hand, the block body records the specific details of the factor information.

4.2. A-MFA Strategy Model. The A-MFA strategy model is an emerging trend that provides a secure way to authenticate. As shown in Table 1, static authentication schemes have limitations in achieving optimal results in dynamic scenarios. Randomly selected authentication schemes face difficulty in measuring available authentication factors accurately. As a result, an adaptive selection algorithm is the

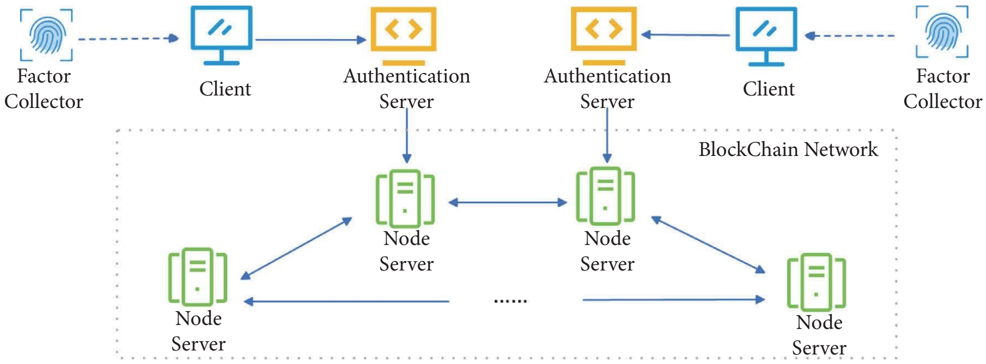

Figure 2: The system model in the blockchain-based authentication scheme.

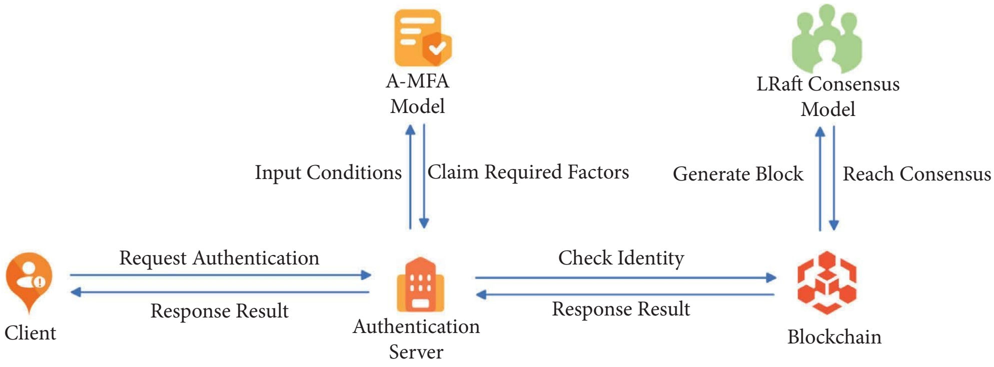

Figure 3: The structure of the blockchain-based authentication scheme.

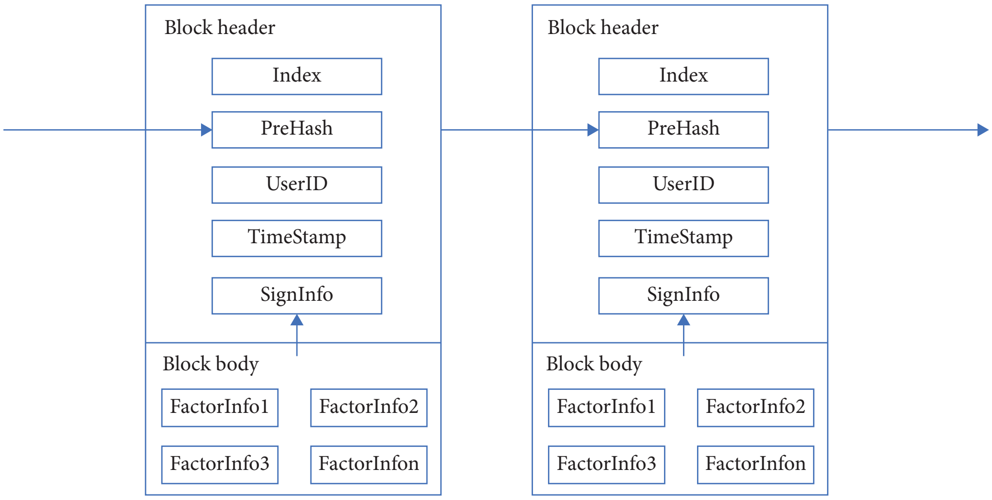

Figure 4: The structure of the blockchain in the proposed scheme.

Table 1: Comparison of different types of authentication schemes.

Authentication schemes		Illustration
Static		A predefined set of schemes for any dynamic environment
Pseudo-static		A fixed solution is dynamically selected in different time scenarios
Dynamic	Random	Schemes are selected randomly during authentication without any predetermined order
	Adaptive	Schemes are selected based on the current system, current environment state, and previous experience patterns

only viable solution to meet these requirements. In this paper, we consider 7 dynamically selectable authentication schemes, including face, fingerprint, password, captcha, SMS, voice, and keystrokes. While some of these scenarios require active user involvement, others can be performed in passive mode. The proposed A-MFA model employs these seven patterns, utilizing different modes for user authentication based on the selection algorithm which uses the genetic algorithm as the evolutionary algorithm. An adaptive selection algorithm optimized by a genetic algorithm is used to calculate the optimal solution, suitable for real-world mobile applications with large and unclear spaces. Genetic algorithms are adept at navigating intricate, expansive, nonlinear, and diverse solution spaces, enabling adaptive decision making that aligns with existing active/continuous MFA systems.

The A-MFA strategy model employs a genetic algorithm for the optimization of authentication schemes. The genetic algorithm offers several advantages for the considered problem, including solution exploration, solution representation, and an evolutionary process. However, we have considered the potential applicability of alternative evolutionary algorithms, such as evolutionary strategies, genetic programming, or particle swarm optimization. In our evaluation of these alternative algorithms, we found that they may not be well suited for our specific problem due to the following reasons:

(1) *Evolutionary Strategies*. These strategies typically rely on real-valued representations and continuous optimization, whereas authentication schemes involve discrete factors and configurations, making evolutionary strategies less suitable for our discrete problem.

(2) *Genetic Programming*. While genetic programming is effective for evolving computer programs or mathematical expressions, its emphasis on program structures may not align well with the specific requirements and constraints of authentication scheme optimization problem.

(3) *Particle Swarm Optimization*. Particle swarm optimization has shown promise in various optimization tasks. However, its effectiveness can be influenced by factors such as swarm size and parameter settings. Moreover, the exploration capability of particle swarm optimization may not be as efficient in our complex search space of authentication factors and configurations.

Considering these factors, we concluded that the genetic algorithm was the most appropriate choice for our research, given its advantages in exploring the solution space, representing authentication schemes, and simulating an evolutionary process.

In this section, we present a micro-genetic algorithm that incorporates a dynamic scheme based on the current device and media settings, varying according to different scenarios. To ensure security, various authentication schemes are stored separately in virtual machines and retrieved from the user console to the server as needed. In order to maintain privacy and security, a multi-factor authentication scheme needs to be updated when a fixed user changes the authentication device or media. This is particularly important when fixed users are in the same operating environment for an extended period of time and face changes in the operating environment or user roles [21]. To address these issues, this section considers three types of devices, i.e., fixed, portable, and handheld, and three types of media, i.e., wired, wireless, and cellular.

One of the main challenges of the proposed design is to establish constraints, objective functions, and penalty functions. The constraints establish the boundaries for various authentication schemes across different devices and media. The objective function is designed to compute the optimal set of solutions with the corresponding tuning parameters, i.e., a subset of the seven modes proposed above. The penalty function is utilized to regulate the selection of authentication schemes to prevent repeated selection of the same scheme at consecutive authentication triggers. To formulate the objective function of any verification scheme, confidence levels are utilized. The confidence levels are expressed as numeric values that indicate how well a particular validation scheme fits into the current environment. A higher level of confidence represents that the authentication scheme is more trustworthy in the current environment. In this study, the value of confidence is determined through an optimization problem, where the confidence level among different devices and media is expressed as a set of constraints using pairwise comparison. The generated decision pairs are then analyzed using stochastic optimization methods, and linear programming is used to solve this problem. In our approach, the constraint function serves as a guiding principle in determining the optimal arrangement of authentication factors from the available set of seven. The constraint function considers all possible combinations of the authentication factors and ranks them based on their trustworthiness values. These values reflect the reliability and effectiveness of each combination in the authentication process. The purpose of the constraint function is to ensure that the selected authentication factors align with the optimization objective of maximizing the overall trustworthiness and effectiveness of the authentication scheme. By prioritizing the combinations based on their trustworthiness values, we can identify the most suitable and reliable configuration of three authentication factors from the available options. The constraint function acts as a constraint within the optimization algorithm, influencing the selection process and guiding the algorithm towards solutions that meet the defined criteria for trustworthiness and effectiveness. It helps ensure that the chosen authentication scheme not only is based on the available devices and media but also considers the trustworthiness of the authentication factors.

The solution employs a dynamic confidence level calculation for three devices and media, effectively addressing the maximum value of the genetic algorithm's objective function. This optimization approach also accommodates the dynamic nature of confidence values and adapts to the constraint sets of various devices and media. For identity ecosystems in different environments, we calculate the confidence level of different task levels and different user types.

The optimization problem can be expressed with various sets of constraints and provide solutions for these problems. When designing the algorithm's objective function, considerations are given to the impacts of the device and media, assigning appropriate weights to produce distinct effects. The form of the objective function is defined as follows:

$$T(M) = \sum_{i=1}^{3}\sum_{j=1}^{3} aX_i + bY_j + c, \tag{1}$$

where a, b, and c are constants, and the weights as variables are adjusted according to different environment settings. X represents the trusted value of the device, and Y represents the trusted value of the media. By weighting the confidence level of the selected pattern, the sum value of the objective function is obtained.

In order for $T(M)$ to choose only three of the seven authentication factors to generate authentication schemes, we introduce additional constraints. One possible approach is to use 0-1 integer programming, where each validating factor has a binary variable that is selected when the variable is 1, and 0 otherwise. Thus, we can convert the original objective function $T(M) = \sum(aX + bY + c)$ into the following form:

$$\begin{aligned} T(M) = {} & aX_1 + bY_1 + cZ_1 + dX_2 + eY_2 \\ & + fZ_2 + gX_3 + hY_3 + iZ_3, \end{aligned} \tag{2}$$

where X_1, Y_1, and Z_1 represent the binary variables of face, fingerprint, and password, respectively; X_2, Y_2, and Z_2 represent the binary variables of captcha, SMS, and voice; X_3, Y_3, and Z_3 represent the binary variables of keystrokes; and $a, b, c, d, e, f, g, h, i$ represent the coefficients corresponding to each verification factor. We then add the following constraints to limit the choice of only three factors:

$$\begin{aligned} X_1 + X_2 + X_3 &= 1, \\ Y_1 + Y_2 + Y_3 &= 1, \\ Z_1 + Z_2 + Z_3 &= 1. \end{aligned} \tag{3}$$

These constraints ensure that only three of the selected factors are 1 and the rest are 0. In this way, we can solve the 0-1 integer programming problem to get the best three authentication factors, thus generating the authentication scheme.

4.3. LRaft Consensus Model. A consortium blockchain is a type of blockchain network that is operated by a group of organizations or entities, rather than being open to the public like a public blockchain. In a consortium blockchain, all participants are carefully selected and entrusted with stringent contractual obligations to ensure their adherence to ethical behavior and maintain a high level of integrity. This type of blockchain architecture is often used in business environments, where the participants have a vested interest in the security and stability of the network. In a consortium blockchain, the consensus mechanism is typically optimized for efficiency and scalability compared to public blockchains, as the number of nodes is predetermined and limited. Consensus algorithms are essential for ensuring the safety and efficiency of distributed systems. The Raft consensus algorithm is a distributed consensus algorithm used for maintaining the consistency of replicated state machines. It is designed to be more understandable than previous consensus algorithms such as Paxos and widely used in distributed systems [22]. Raft is designed with simplicity in mind, making it easier to understand, implement, and maintain compared to more complex consensus algorithms. The algorithm's clear separation of roles and its emphasis on leader-based replication greatly simplify the consensus process. Raft incorporates an efficient leader election mechanism, which ensures the selection of a leader with the most up-to-date log. This approach minimizes the chances of split votes or stale leaders, leading to more efficient and reliable consensus. Raft places a strong emphasis on safety and availability. The algorithm guarantees that a majority of the nodes need to agree on a log entry before it is committed, ensuring data consistency and reliability. Additionally, Raft can tolerate network partitions and node failures, allowing the system to maintain availability even in the presence of disruptions.

In the Raft algorithm, nodes operate in three distinct states: leader, follower, or candidate. Time is divided into terms, each with a fixed duration. At the start of each term, an election takes place where one or more candidates vie to become the leader. If a candidate emerges as the winner, they assume the role of leader for the duration of the term [23]. The complete conversion process is shown in Figure 5. The Raft algorithm is known for its simplicity and high efficiency and is widely used in practical systems.

The LRaft consensus model is a variant of the Raft algorithm which is designed based on the following conditions:

(1) All nodes in the consensus group have the potential to become leaders in Raft. However, in order to improve election efficiency and ensure that only a few pivotal nodes are responsible for the critical function of authentication, the number of participating nodes in the election is decreased. The remaining nodes are responsible for secondary functions, such as block verification and message transmission.

(2) The original Raft model has weak fault tolerance in which the leader nodes maintain accounting and new elections are only carried out when the node fails, making it vulnerable to single point of failure and attacks against critical nodes. To improve fault tolerance, LRaft introduces mechanisms like random leaders and node classification.

In the LRaft consensus algorithm, there are two types of nodes: ordinary nodes that act as followers and authoritative nodes that act as potential leader candidates, as shown in

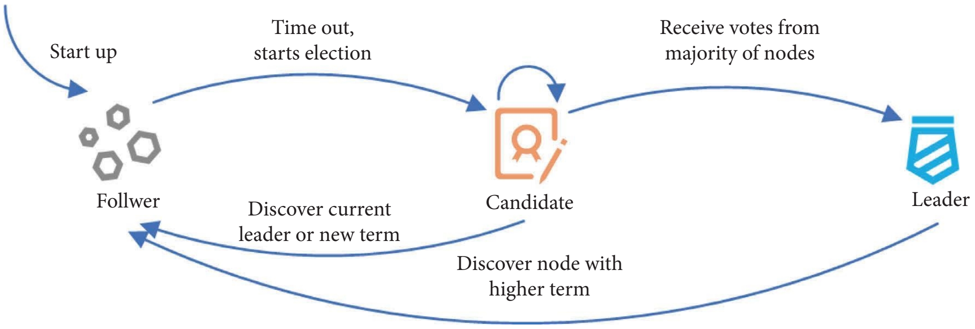

Figure 5: The role transition process of Raft.

Table 2. The follower is identified with a flag bit of 0 and is primarily responsible for transmitting messages and continuously verifying blocks to ensure the integrity of system. The candidate, which uses a flag bit of 1, is a group of preset authoritative nodes that participate in block verification and the consensus process. The leader node, identified by a flag bit of 2, is the winner elected by the candidate group and is responsible for generating blocks and participating in the consensus process. It is worth noting that the leader is actually included in the candidate group. In LRaft, the follower and candidate nodes play distinct roles in the consensus algorithm, ensuring the security and reliability of the system.

The state transition is illustrated in Figure 6. In LRaft, only authoritative nodes in the consensus group have an opportunity to become leaders, which are expected to master the critical function of authentication. The other nodes are responsible for secondary functions such as verifying blocks and transmitting messages. To prevent attackers from guessing the processing node, each request in the proposed authentication scheme is handled by a different leader node. During the block production cycle, a new leader is elected to be responsible for generating blocks, and the term is determined based on the block interval. As shown in Algorithm 1, during the initialization phase, all trusted nodes within the specific group are in the candidate state and have their timeout timers randomly set. Meanwhile, the follower nodes remain in a sleeping state. The candidate initiates a vote request from other nodes, and upon receiving votes from over half of the nodes, it becomes the leader for the current term. By randomly selecting the leader node and handling each request by a different leader node, the LRaft consensus model ensures a higher level of security and prevents attackers from targeting a specific processing node.

4.4. Workflow of Proposed Authentication Scheme. In this section, we describe the identity authentication process of the proposed scheme, which includes two phases as follows.

Table 2: Flags and responsibilities of nodes with different roles.

Roles	Flag bit	Responsibilities
Follower	0	Transmit messages and verify blocks
Candidate	1	Verify blocks and participate in consensus
Leader	2	Generate blocks and participate in consensus

4.4.1. The User Registration Phase. Before authentication, users must store authentication information within the blockchain. The registration process is described as follows:

Step 1. The User_i inputs the identity ID_i and collects the set of authentication factors $W = \{w_1, w_2, \ldots, w_n\}$ through the factor collector.

Step 2. The Client called ReqNode combines the information of the user and sends a request $Request\_of\_$ $\text{Registeration}\{ID_i, \text{TimeStamp}, W, \text{ReqNode}\}$ to the blockchain.

Step 3. The follower node broadcasts the pending message to the blockchain. A leader node will be elected through LRaft consensus algorithm. After election, the leader node broadcasts the user registration request to the blockchain, and other nodes perform blockchain backtracking, respectively, to check whether the user has registered. The response to check result is $\text{Response\_of\_CheckReg}\{ID_i, \text{Bool}\}$.

Step 4. After receiving responses from more than half of the nodes, the leader node confirms that the user has not registered and packs user information into a block. At the same time, the leader node will generate a pair of keys named PU_k and PR_k through the RSA algorithm, and the SignInfo is calculated as follows:

$$\text{SignInfo} = \text{PR}_k\left(\text{Hash}\left(\text{Merkel}\left(w\right)\right)\right). \tag{4}$$

Hash ( ) indicates the SHA256 algorithm and Merkle ( ) indicates the result of the hash tree, which can be used to verify any kind of data stored, handled, and transferred in the blockchain. In addition, BlockHash written into BlockHeader is calculated as

$$\text{BlockHash} = \text{Hash}\left(\text{PreHash} + \text{TimeStamp} + ID_i + \text{SignInfo}\right). \tag{5}$$

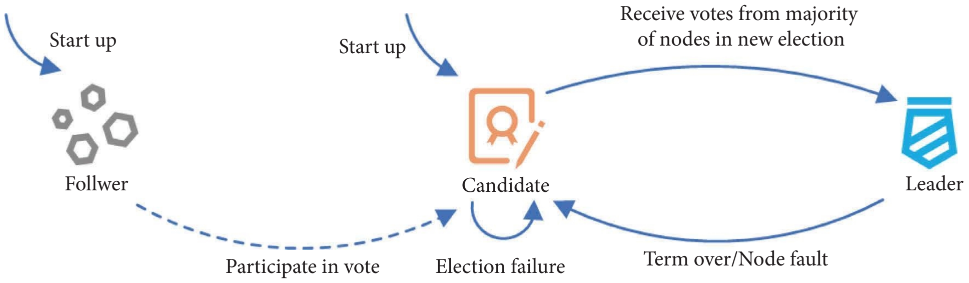

FIGURE 6: The process of three role transitions after modifications to the Raft algorithm.

```
Input: The nodes participating in consensus $\{\text{Node}_n \mid n \in \text{Num}\}$, the number of nodes Num, follower node set $F$, Candidate set $C$,
Timeout_Max $T$
Output: Leader $\text{Node}_i$
Initialization:
//Initializing the blockchain and flags for follower nodes and candidate nodes
(a) For follower node in $F$, flag = 0. For candidate node in $C$, flag = 1.
(b) For node in $\text{Node}_n$, set the initial BlockIndex = 0
Procedure:
while receive request from user or detect the failure of Leader do:
    //Start new election
  (I) For candidate nodes:
    for $\forall c \in C$;
      Set timeout ($T$)
    //Election timeout occurs, candidate nodes invite votes to win the election
    if timeout do:
      RequestVote ($C_i$, $C_i$.BlockIndex)
    end if
  (II) For follower nodes:
    while ReceiveRequestVote ($C_i$, $C_i$.BlockIndex) do:
      //Check whether the candidate node is legitimate and has the latest blockchain status
      if $C_i$ in $C$ and $C_i$.BlockIndex > = $F_j$.BlockIndex do:
        SendVote ($F_j$, $C_i$)
      else do:
        RefuseVote($F_j$, $C_i$);
      end if
  (III) For leader node:
    if winElection() do:
      //The Leader node performs the block generation operation.
      BecomeLeader (Node $ID$)
      flag = 2
      GenerateNewBlock()
      SendCommitMessage()
    end if
  end while
return Leader $\text{Node}_i$
```

ALGORITHM 1: The election algorithm of LRaft.

Step 5. After the Leadr Node builds the block, a message will be broadcast to the blockchain Commit_ of_Registeration $\{ID_i, \text{BlockIndex}, \text{TimeStamp}, \text{BlockHash}, \text{Leadr Node}\}$, and the other nodes begin to synchronize the block.

Step 6. The requested node returns the symmetric public key (PU_k) of the private key (PR_k) to the user Response_of_Registeration$\{ID_i, \text{Bool}, \text{Cert}_{PU_k}\}$ as one of the credentials for future identity verification.

4.4.2. The User Authentication Phase. The authentication process is described as follows:

Step 1. When a User_x requests authentication, the requested server will detect the user's operating environment. After that, the server informs the user of the required authentication factor group in conformity with the calculation result of the A-MFA strategy model, which is List_of_Needed Factor $\{w_1', w_2', \ldots, w_n'\}$.

Step 2. The user sends the authentication information and credentials according to the requirements of the server. We can express this process as

$$\text{Request\_of\_Authentication}\{ID_x, \text{List\_of\_Needed Factor}, \text{Cert}_{PU\_k}\}. \quad (6)$$

Step 3. The follower node broadcasts the pending message to the blockchain. A leader node will be selected through a consensus algorithm. After the election is completed, the leader node requires other nodes to perform blockchain backtracking, respectively, and find the latest block to check whether the user exists by checking if there exists a SignInfo in the block header that can be decrypted using PU_k. The response is Response_of_Check User Exist$\{ID_x, \text{Bool}\}$.

Step 4. When more than half of the nodes confirm that the user exists, then all nodes will verify whether the authentication factor set List_of_Needed Factor submitted by the user meets the authentication requirements.

Step 5. When more than half of the nodes confirm that the user is legitimate, the leader node will generate a new pair of keys named PU_k' and PR_k' and calculate SignInfo with PR_k' again.

Step 6. The leader node broadcasts the commitment message to the blockchain, which is Commit_of_ Authentication $\{ID_i, \text{BlockIndex}, \text{TimeStamp}, \text{BlockHash}, \text{Leadr Node}\}$, and other nodes will synchronize the block.

Step 7. The requested node returns Response _of_Authentication$\{ID_x, \text{Bool}, \text{Cert}_{PU_k'}\}$ to the user.

5. Results and Discussion

This section presents a comprehensive security analysis of the proposed scheme. We conduct a series of experiments to evaluate the efficiency and effectiveness of our scheme.

5.1. Security Analysis

5.1.1. Resistance to Brute Force Attacks. Brute force attacks are a type of cyberattack where an attacker tries to guess a password or encryption key by systematically trying every possible combination of characters until the correct one is found. In the proposed scheme, each authentication requires the user to obtain a one-time authentication credential Cert_{PU_k} generated by the leader node and returned to the user for safekeeping at each verification or registration. As a result, an attacker cannot attempt to brute force a user's password or biometrics because they do not have direct access to these authentication credentials. Even if the attacker obtained a user's one-time authentication credential, it would be useless as it is valid only for a single authentication attempt and would expire after use. Therefore, the blockchain-based MFA scheme can effectively resist brute force attacks.

5.1.2. Resistance to Guessing Attacks. A guessing attack is a type of attack in which an attacker tries to guess the correct authentication factor set of a user. In the proposed scheme, the adaptive multi-factor selection model dynamically generates the user's authentication factor set $W = \{w_1, w_2, \ldots, w_n\}$ based on factors such as devices and media, making the selection process more complex and less predictable for the attacker. Furthermore, each authentication requires the user to provide authentication credentials Cert_{PU_k} or biometrics which are unique and not easily guessable. Overall, it is highly resistant to guessing attacks.

5.1.3. Resistance to Replay Attacks. A replay attack is a type of attack where an attacker captures a valid message sent between two parties and then replays it to perform some unauthorized action. In the proposed scheme, the authentication process is resistant to replay attacks due to the use of the One Time Password (OTP) Cert_{PU_k} generated by the leader node. The OTP is a time-based authentication certificate that is updated by the accounting node at each block interval. When a user requests authentication, the leader node will retrieve the latest matching block from the blockchain to verify the user's OTP. If the OTP has been used previously or does not match, the authentication will fail. This prevents an attacker from replaying a previously used OTP to gain unauthorized access to the system.

5.1.4. Resistance to the Single Point of Failure. In the proposed scheme, the resistance to a single point of failure is achieved through the use of a consensus algorithm and a distributed network of nodes. The authentication process is decentralized and distributed among the nodes in the network. If one node in the network fails, the other nodes in the network can continue to function and maintain the network's integrity. In addition, the consensus algorithm LRaft used in the blockchain-based MFA scheme ensures that a new leader node is elected in the event of a failure, further increasing the system's resiliency to single points of failure.

5.1.5. Resistance to Conspiracy Attacks. Conspiracy attacks occur when an attacker colludes with a trusted node or insider to impersonate a legitimate user and gain unauthorized system access. To counter such attacks, the proposed scheme utilizes a consortium blockchain architecture, where a group of trusted entities follows strict contractual obligations for proper behavior. The user's authentication information remains private, posing a challenge for attackers attempting to impersonate legitimate users. Even if an attacker colludes with one of the nodes to pass

Table 3: Comparison of the proposed scheme with other schemes.

Security features	Yao et al. [24]	Masud et al. [25]	Bao and You [26]	Proposed
Resistance to brute force attack	√	√	√	√
Resistance to guessing attack	√	×	×	√
Resistance to replay attack	√	√	×	√
Resistance to the single point of failure	×	×	√	√
Resistance to conspiracy attack	×	√	√	√
Mutual dynamic authentication	√	√	√	√
Consistency of public information	×	×	√	√

illegal verification, they cannot guarantee that the node will be elected as the leader node within the block generation interval. Furthermore, since verification is passed by multiple nodes, any illegal verification attempts can be easily detected. Similarly, an attacker cannot pretend to be a blockchain node, especially the leader node, because the trusted node set C is initially limited.

5.1.6. Mutual Dynamic Authentication. In a blockchain-based MFA scheme, mutual dynamic authentication can be achieved through the interaction between the user and the authentication server. When a user sends a verification request to the blockchain network, any node that receives the request will first query its local user information table to find the corresponding block. The user's legitimacy is then verified by comparing the multi-factor information $W = \{w_1, w_2, \ldots, w_n\}$ stored in the block with the user's submitted identity information. As for the authentication of the user to the blockchain, the scheme uses the consortium chain architecture. Each node in the blockchain has a unique ID for identification, and the network cannot be joined arbitrarily. Moreover, each consensus process will use the private key of the leader node to sign the message. The user can use verify the corresponding signature to complete the authentication to the blockchain.

5.1.7. Consistency of Public Information. The consensus algorithm ensures agreement among blockchain nodes, guaranteeing data consistency in the blockchain ledger. The distributed storage and high redundancy in the blockchain make data tampering challenging, as any tampering will be detected during the next consensus process. Therefore, once public information is recorded on the blockchain, the user's corresponding public information used in authentication remains consistent with the information extracted during registration.

Table 3 shows that the proposed scheme is more secure and more functional than the current schemes. Yao et al. [24] and Masud et al. [25] both implemented centralized server-based authentication schemes, relying on cryptographic techniques such as hashing and homomorphic encryption to ensure the confidentiality and reliability of the authentication process. However, these schemes are vulnerable to single points of failure and collusion attacks by internal personnel. Additionally, they do not guarantee the integrity and protection of data against malicious tampering and destruction.

On the other hand, Bao and You [26] introduced a blockchain-based architecture for authentication, which provides improved security. This idea aligns well with the approach we proposed. However, the scheme in [26] utilizes fuzzy extractors to store users' two-factor authentication information within the blockchain, without considering the fact that storing users' identity information within the blockchain makes it susceptible to malicious attackers who can easily steal and launch impersonation and replay attacks. In the proposed scheme, we mitigate such attacks by introducing the user identity authentication credential ($\mathrm{Cert}_{PU'_k}$).

5.2. Effectiveness Evaluation of A-MFA Strategy Model. In this section, we conduct experiments to test the proposed A-MFA selection framework with different device and media combinations. The genetic algorithm used in the experiment adopts the NSGA-II algorithm [27], which supports the search for an approximate optimal solution in a multi-objective problem. The weight values of the devices and media shown in (1) are set in the experiment. Some of the device and media combinations tested include equal weight for devices and media, greater weight for media than devices, and greater weight for devices than media. Figure 7 shows the authentication mode selected by devices and media when events are triggered at different times under the scenario of equal weight.

Figure 7 illustrates that different trigger events result in unique authentication factor combinations, ensuring diverse selection decisions. This robustness makes it challenging for attackers to identify any selection patterns, even in a stable environment over time. Comparing the adaptive selection method to random selection and optimal cost selection, the adaptive selection consistently outperforms the other two approaches in all trigger events.

5.3. Efficiency Evaluation of LRaft Consensus Model. In this section, we pay attention to the efficiency of the proposed authentication scheme. The multi-factor authentication strategy model determines the accuracy of authentication, and the consensus algorithm determines the efficiency.

In the simulation tests, the hardware system used is an Intel(R) Core(TM) i7-8700 3.20 GHz processor with 16 GB DDR4-2666 dual-channel memory. The operating system platform used was Kali 2018.2 AMD 64. The simulation tool utilized is the MPICH-3.2.1 Concurrency package involving a complete node simulation. We consider a distributed network with N nodes where there are n highly trusted

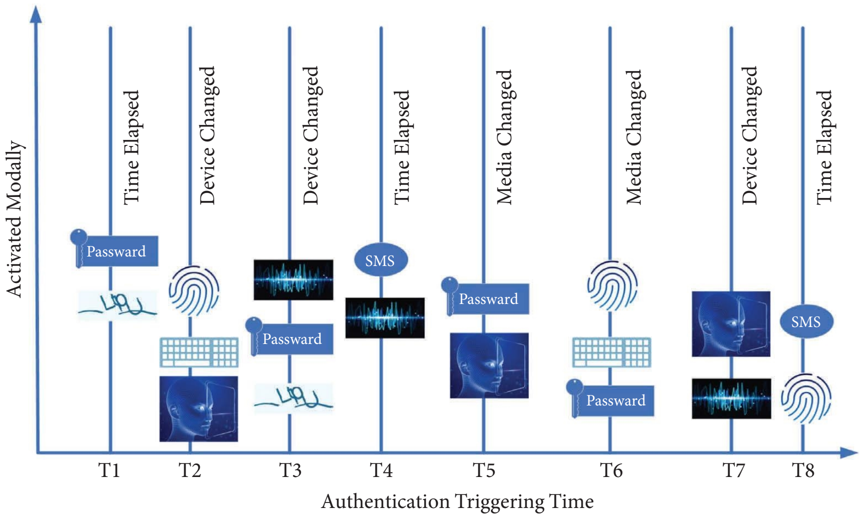

Figure 7: Multiple modality selections under diverse triggering events.

Table 4: Leader election time of LRaft consensus algorithm.

T (ms)/nodes	10	20	40	60	80	100
Raft	0.016384	0.018452	0.021762	0.031093	0.563240	0.094892
Proposed	0.004905	0.008329	0.014903	0.016231	0.018891	0.020386

nodes. Nodes communicate with each other following the Raft algorithm. The election timeout is randomly set between 100 ms and 200 ms. By changing the number of clusters N and the number of authoritative nodes n, we observe the leader election time to reflect the system's efficiency. We simulate 10 rounds of elections from 10 nodes to 100 nodes, where the proportion of authoritative nodes is 1/5, and record the time T it spent to elect the leader. The detection time is the time between the candidate node starting to send the invitation information T_1 and the leader node elected T_2:

$$T = T_2 - T_1. \tag{7}$$

The effectiveness and optimization of LRaft are demonstrated by comparing it with the original Raft algorithm as shown in Table 4. The data in the table are the average of ten simulation results.

As shown in Table 4, a larger number of nodes lead to an increase in the time required for leader election. However, compared with the original Raft algorithm, our proposed consensus model shows strengths in efficiency because of the limitation of the number of nodes participating in the election, thereby helping to improve the efficiency of the scheme. Meanwhile, this can also avoid the adverse effects of malicious nodes on the system.

6. Conclusions

Nowadays, centralized server-based authentication schemes pose significant security challenges, including single-point failure, the exposure of personal information, and the risk of identity theft. Moreover, the static and single-factor authentication methods cannot provide adequate protection for computing devices and applications, which is a major challenge in today's security landscape. To address these challenges, this paper proposes a blockchain-based authentication scheme with an adaptive multi-factor selection strategy. The proposed scheme includes a blockchain-based authentication framework, an adaptive multi-factor authentication strategy model, and a consensus model named LRaft for rapid and secure authentication. The proposed scheme has been extensively evaluated for resistance against simulated attacks and shown to be highly effective and efficient. The results have confirmed the efficacy of the proposed scheme, which offers a secure, decentralized, and flexible solution for authentication in dynamic mobile applications.

Data Availability

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

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the National Key Research and Development Program of China (grant no. 2020YFB1805400) and the Sichuan Science and Technology Program (grant nos. 2022YFG0193 and 2023YFG0113).

References

[1] I. Velásquez, A. Caro, and A. Rodríguez, "Authentication schemes and methods: a systematic literature review," *Information and Software Technology*, vol. 94, pp. 30–37, 2018.

[2] A. Peterson, E. Yahr, and J. Warrick, *Leaks of Nude Celebrity Photos Raise Concerns about the Security of the Cloud*, The Washington Post, Washington, DC, USA, 2014.

[3] M. Belotti, N. Božić, G. Pujolle, and S. Secci, "A vademecum on blockchain technologies: when, which, and how," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3796–3838, 2019.

[4] T. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang, "Untangling blockchain: a data processing view of blockchain systems," *IEEE Transactions on Knowledge and Data Engineering*, vol. 30, no. 7, pp. 1366–1385, 2018.

[5] 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.

[6] S. Ai, D. Hu, and J. Guo, "Distributed multi-factor electricity transaction match mechanism based on blockchain," in *Proceedings of the 2020 IEEE International Conference on Energy Internet*, pp. 121–127, Sydney, NSW, Australia, August 2020.

[7] S. Guo, X. Hu, S. Guo, X. Qiu, and F. Qi, "Blockchain meets edge computing: a distributed and trusted authentication system," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 1972–1983, 2020.

[8] D. Zhang, F. R. Yu, and R. Yang, "Blockchain-based multi-access edge computing for future vehicular networks: a deep compressed neural network approach," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 8, pp. 12161–12175, 2022.

[9] Y. Xu, Y. Meng, and H. Zhu, "An efficient double-offloading biometric authentication scheme based on blockchain for cross domain environment," *Wireless Personal Communications*, vol. 125, no. 1, pp. 599–618, 2022.

[10] Y. Zhang, B. Li, J. Wu, B. Liu, R. Chen, and J. Chang, "Efficient and privacy-preserving blockchain-based multi-factor device authentication protocol for cross-domain IIoT," *IEEE Internet of Things Journal*, vol. 9, no. 22, pp. 22501–22515, 2022.

[11] H. Wang, X. Zhang, Y. Xia, and X. Wu, "An intelligent blockchain-based access control framework with federated learning for genome-wide association studies," *Computer Standards & Interfaces*, vol. 84, Article ID 103694, 2023.

[12] X. Wu, H. Wang, Y. Zhang, and R. Li, "A secure visual framework for multi-index protection evaluation in networks," *Digital Communications and Networks*, vol. 9, no. 2, pp. 327–336, 2023.

[13] X. Wu, Y. Zhang, M. Shi, P. Li, R. Li, and N. N. Xiong, "An adaptive federated learning scheme with differential privacy preserving," *Future Generation Computer Systems*, vol. 127, pp. 362–372, 2022.

[14] W. Li, H. Cheng, P. Wang, and K. Liang, "Practical threshold multi-factor authentication," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 3573–3588, 2021.

[15] M. Calvo and M. Beltrán, "A Model for risk-Based adaptive security controls," *Computers & Security*, vol. 115, Article ID 102612, 2022.

[16] D. Dasgupta, A. Roy, and A. Nag, "Toward the design of adaptive selection strategies for multi-factor authentication," *Computers & Security*, vol. 63, pp. 85–116, 2016.

[17] A. Wójtowicz and K. Joachimiak, "Model for adaptable context-based biometric authentication for mobile devices," *Personal and Ubiquitous Computing*, vol. 20, no. 2, pp. 195–207, 2016.

[18] A. Roy and D. Dasgupta, "A fuzzy decision support system for multifactor authentication," *Soft Computing*, vol. 22, no. 12, pp. 3959–3981, 2018.

[19] A. Hassan, B. Nuseibeh, and L. Pasquale, "Engineering adaptive authentication," in *Proceedings of the 2021 IEEE International Conference on Autonomic Computing and Self-Organizing Systems Companion*, pp. 275–280, DC, USA, September 2021.

[20] M. Calvo and M. Beltrán, "A model for risk-based adaptive security controls," *Computers & Security*, vol. 115, Article ID 102612, 2022.

[21] A. K. Nag, A. Roy, and D. Dasgupta, "An adaptive approach towards the selection of multi-factor authentication," in *Proceedings of the 2015 IEEE Symposium Series on Computational Intelligence*, pp. 463–472, Cape Town, South Africa, December 2015.

[22] B. Rong and Z. Zheng, "FRCR: Raft consensus scheme based on semi asynchronous federal reconstruction," *IEEE Transactions on Network and Service Management*, vol. 19, no. 4, pp. 3822–3834, 2022.

[23] Y. Abuidris, R. Kumar, T. Yang, and J. Onginjo, "Secure large-scale E-voting system based on blockchain contract using a hybrid consensus model combined with sharding," *ETRI Journal*, vol. 43, no. 2, pp. 357–370, 2021.

[24] M. Yao, X. Wang, and Q. Gan, "An improved and privacy-preserving mutual authentication scheme with forward secrecy in VANETs," *Security and Communication Networks*, vol. 2021, Article ID 6698099, 12 pages, 2021.

[25] M. Masud, G. S. Gaba, K. Choudhary, M. S. Hossain, M. F. Alhamid, and G. Muhammad, "Lightweight and anonymity-preserving user authentication scheme for IoT-based healthcare," *IEEE Internet of Things Journal*, vol. 9, no. 4, pp. 2649–2656, 2022.

[26] D. Bao and L. You, "Two-factor identity authentication scheme based on blockchain and fuzzy extractor," *Soft Computing*, vol. 27, no. 2, pp. 1091–1103, 2021.

[27] K. Deb, A. Pratap, S. Agarwal, and T. Meyarivan, "A fast and elitist multiobjective genetic algorithm: nsga- ii," *IEEE Transactions on Evolutionary Computation*, vol. 6, no. 2, pp. 182–197, 2002.