Hindawi
Mathematical Problems in Engineering
Volume 2021, Article ID 5058780, 12 pages
https://doi.org/10.1155/2021/5058780

Research Article

Secure Online Examination with Biometric Authentication and Blockchain-Based Framework

Xiaoling Zhu [1] **and Chenglong Cao** [2]

[1]*School of Computer Science and Information Engineering, Hefei University of Technology, Hefei 230601, China*
[2]*Anhui Finance and Trade Vocational College, Hefei 230601, China*

Correspondence should be addressed to Xiaoling Zhu; zhuxl@hfut.edu.cn and Chenglong Cao; chenglongcao@sina.cn

Received 3 June 2021; Revised 11 August 2021; Accepted 17 August 2021; Published 26 August 2021

Academic Editor: Jude Hemanth

E-learning has been carried out all over the world and then online examinations have become an important means to check learning effect during the outbreak of COVID-19. Participant authenticity, data integrity, and access control are the assurance to online examination. The existing online examination schemes cannot provide the protection of biometric features and fine-grained access control. Particularly, they did not discuss how to resolve some disputes among students, teachers, and a platform in a fair and reasonable way. We propose a novel biometric authentication and blockchain-based online examination scheme. The examination data are encrypted to store in a distributed system, which can be obtained only if the user satisfies decryption policy. And the pieces of evidence are recorded in a blockchain network which is jointly established by some credible institutions. Unlike other examination authentication systems, face templates in our scheme are protected using a fuzzy vault and a cryptographic method. Furthermore, educational administrative department can determine who the real initiator of malicious behavior is when a dispute arises using a dispute determination protocol. Analysis shows that no central authority is required in our scheme; the collusion of multiple users cannot obtain more data; even if the authorities compromise, biometric features of each user will not be leaked. Therefore, in terms of privacy-preserving biometric templates, fine-grained access, and dispute resolution, it is superior to the existing schemes.

1. Introduction

Owing to the outbreak of COVID-19, online teaching and learning has been carried out all over the world. Network and communication technology guarantees the fluency of online teaching process. Cloud computing provides storage and processing ability of massive data. Internet of things makes data retrieval easier through mobile phones, laptops, and PC. E-learning environment has been improved, and education boundary has been greatly widened [1]. In China, some platforms provide convenient and diversified interfaces. For example, Tencent Classroom provides online teaching services, and Rain Classroom provides online examination functions.

As a result, online examinations are becoming more and more important. It generally includes the following phases: issuing test papers, participating in the examination, submitting answer papers, scoring the papers, and publishing the scores. During the phases, to maximize scores to obtain higher course credits, some users might initiate deception attacks, such as the leakage and tampering of test papers, the impersonation to participate in examination, and the tampering of answer sheets after submission. So, the security of online examination should draw enough attention.

Authentication is widely used in online examinations. There are three ways for authentication [2]: (i) knowledge based. It requires a user to provide what he knows (e.g., a password); (ii) token based. It requires a user to show what he owns (e.g., mobile device and token); (iii) biometrics (e.g., fingerprints and human faces). Among the methods, password is the most widely used. But, if one person tells his password deliberately to someone else, impersonation will happen. If biometric authentication is used, the disclosure of

biological templates will lead to serious security and privacy problems.

Moreover, if examination data are put in the cloud, some measures should be taken to prevent the data from being illegally modified and damaged [3, 4]. To build an open and tamper-resistant e-learning environment, some works have turned to the blockchain technology to construct a shared, distributed, and fault-tolerant database [5, 6]. Data sharing brings some conveniences to learners, institutions, and employers [7, 8]. Professor John Domingue, director of the Knowledge and Media Research Center of the Open University in the United Kingdom, believed that blockchain and smart contracts would cater to the increasingly decentralized learning pattern [9]. Considering that the data in the public ledger of blockchain are accessed by each user, access control should be considered. In addition, when a dispute between users occurs, it requires a manager to make a reasonable judgment. However, pervious works [10–13] did not consider fine-grained access control, biometric template protection, and dispute resolution.

More specifically, a possible scene is shown in Figure 1. A teacher releases the test papers. Students participate in the examination and submit their answer sheets. The teacher downloads and reviews the answer sheets. Then, the students query their scores. In the system, teachers, students, and a platform have different security requirements. For the platform, he worries that illegal users invade the system; he expects that the students can view their course papers and the teacher can view the answer sheet about his course. For the teacher, he is worried whether test papers, answer sheets, and the scores have been tampered with; he expects that cheating behaviors, such as a second submission, can be found. For students, he worries about other things. For example, are his scores reasonable? Are his biometric templates leaked? Does someone impersonate him to participate in an examination?

For students, teachers, and the platform, their common concern is whether educational administration department can make a reasonable judgment on disputes. For example, a teacher asks students to submit answer sheets and related materials in a compressed form within the time allowed. Then the teacher issues the course scores, a student is not satisfied with his score and then makes an appeal to the administration. Next, the teacher downloads the compressed package and checks it again. To his surprise, the compressed package is different from the previously downloaded version. Who is responsible for the event?

In this paper, we propose a novel online examination scheme with biometric authentication and blockchain-based framework (SEBB) to solve the problems of privacy-preserving biometric templates, fine-grained access, and dispute resolution. The main contributions of this work can be summarized as follows:

(i) Compared with password authentication, our method needs to brush face to complete authentication without inputting a password from the keyboard, which improves the convenience of the system. But in a traditional biometric authentication, biological template is not protected. In SEBB, the method of combining biometrics and cryptography is adopted where face features are extracted with random points together to form a fuzzy vault. Since the biometric template is protected by a fuzzy vault, the risk of template leakage is greatly reduced.

(ii) Fine-grained configuration mechanism of access rights for examination data is designed. The system is composed of students, teachers, educational administrative department, and online platform. They must register to obtain their own keys from the authorities. All elements in the online exam, such as test papers, answer sheets, and scores, are designated to the access policies by the data owners. The attribute-based encryption method is used, and the ciphertext data are stored in a distributed storage system. Only the persons who meet the policies can access the data. It ensures that examination content is confidential and the access is authorized. In addition, attribute keys are distributed by multiple authorities in SEBB, which avoids a single point of failure.

(iii) Examination data and evidence data are integrated for digital forensics. In SEBB, the institutions with high credibility jointly establish a consortium blockchain to record the evidence of uploaded data. Blockchain ensures that the uploaded data can be verified and tamper attacks can be found. When a dispute arises among students, teachers, and the platform, educational administrative department can extract the data in a distributed storage system and the evidence from the blockchain, check data consistency, and then make a judgment.

Our work provides a trusted framework for online examinations. It is conducive to protecting examination data against tampering and eavesdropping and promoting education fair. The remainder of this paper is organized as follows. First, we introduce related works in section 2, which will emphasize the motivation of our work. We then describe system model, security model, and design objectives in section 3 and propose the SEBB scheme in details in section 4. We analyze security and performance in sections 5 and 6, respectively. Finally, we conclude the paper in section 7.

2. Literature Review

Online examination system allows an institute to arrange, conduct, and manage examinations via an online environment. It assists the inspector with reducing the work of leading exam, checking answer sheets, and producing result [14]. So, online exams have gained a lot of popularity in the past few years. Okada et al. [15] pointed out that although a lot of young students share their personal data in their social networks, in the context of e-assessment, their attitude is different because they are more concerned about data privacy, security, and safety.

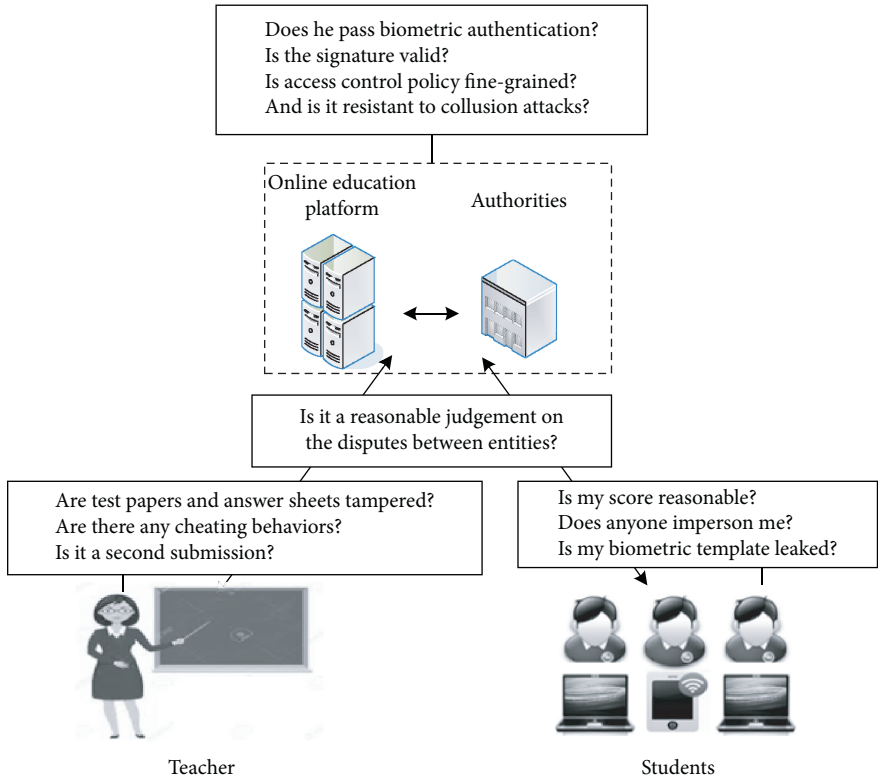

Figure 1: A possible scene.

2.1. User Authentication. The authentication of user digital identities is important for reducing cheating in online examination. In general, password authentication may be broken by brute force because a password with 6 to 8 characters is short and lacks randomness. Meanwhile, biometric features of different persons are different; the features extracted by the same person at different times are not different; so biometric features have better randomness. A general biometric system aimed at capturing facial or fingerprint features [16]. In other cases, multiple biometrics were combined, such as face with fingerprint, fingerprint with mouse patterns [17], and fingerprint with vocal traits [18]. Fenu et al. [19] attempted to verify student identity by performing a fusion of different biometric responses (face, voice, touch, mouse, and keystroke) based on the device and the interaction. Saleem and Haneef [20] incorporated the traditional username/password technique to the palm-based biometric authentication technique, and the examinee was continuously monitored by a webcam to get the optimum security during the exam. Secure testing browsers and camera monitoring have been used at Harvard School of Dental Medicine during remote virtual examinations. Through the questionnaire of the examiners, Kaczmarek et al. [21] found a few clear trends emerge: camera monitoring can be detrimental as it produces higher levels of anxiety. The schemes [16–21] focused on biometric authentication and online exam supervision. However, they did not discuss the protection of biometric features. If the features are leaked, the attacker will probably restore the original image from the template and pass the authentication.

2.2. Data Confidentiality. In an e-learning system, data cannot be known to unauthorized users. If a teacher uploads the exam data, the data can only be accessible for authenticated and authorized students. Encryption is a popular method for access control. Kausar et al. [22] presented a session key establishment protocol for a specified time period such as a class, a seminar, or an exam; public key infrastructure was used to distribute session key which encrypts messages using symmetric cryptography algorithm; the hash-based message authentication code was used for message integrity. In Al-Hawari and Alshawabkeh's study [23], the students are required to correctly enter the provided exam instance session password to successfully complete the login process; an exam instance session password was automatically generated by the examination management system and was only disclosed by the instructor at the beginning of the corresponding session. In few previous studies [22, 23], a single-point failure may occur; repudiation behaviors of communicating parties cannot be avoided; the disputes among internal members cannot be settled. Sahaya et al. [24] proposed a model that encrypts the message using DES and then encodes the encrypted message using Reed Solomon code in the data centers, which is an effective way of uploading and downloading data in cloud-based systems. But it lacks fine-grained access control.

2.3. Blockchain-Based Online Education. Rashid et al. [10] proposed a platform for funding needy students based on the concept of blockchain technology. Palma et al. [11]

presented an implementation for the digitization of degree certificates and academic credits for higher education in the Brazilian education system with smart contracts. Rahman et al. [25] provided a new proposal of devising a security and privacy-preserving design mechanism of data transactions in educational microservices leveraging the blockchain technology, which has high survey acceptance in terms of confidentiality, integrity, and availability. Deenmahomed et al. [26] focused on the design and implementation of an examination, transcript, and certificate system using blockchain, where credits transaction is created when a student completes a course, and a mobile wallet is provided to allow students to have a copy of their certificates. With the help of blockchain, previous studies [10, 11, 25, 26] provided security mechanisms, such as tamper proof.

Previous schemes [16–21], based on biometric authentication, did not discuss the protection of biometric features. Previous studies [22, 23] cannot avoid single-point failures. Previous literature [10, 11, 25, 26] cannot provide fine-grained access control. We focus on authentication, confidentiality, and tamper proof in designing an online examination scheme. And it is superior to the existing schemes in terms of privacy-preserving biometric features, fine-grained access control, avoidance of single-point failure and dispute resolution.

3. Problem Statement

The section provides system model, security model, and design objectives.

3.1. System Model. We adopt consortium blockchain to establish SEBB. Six types of entities are included as follows (Figure 2), and the notations are described in Table 1.

(1) Data providers upload data before the specified time. They may be students or teachers. Students submit answers, and teachers submit scores. Data are stored in ciphertext in a distributed storage system, and its evidence is stored in the blockchain.

(2) Data requestors obtain data from the platform. The requestors include students, teachers, and educational administration departments.

(3) Blockchain nodes are built and maintained by several institutions with high credibility, such as educational administration departments and educational alliances. They record the pieces of evidence of the uploaded data.

(4) Distributed storage system (DSS) is used to store encrypted data.

(5) Online education platform (EP) provides various service interfaces such as online classroom and examination.

(6) Authorities include key distribution authority (KA), registration authority (RA), authentication authority (AA), and educational administration departments (EA). KAs are responsible for key distribution after inspection. AAs are in charge of identity authentication when users login. EAs deal with examination affairs and disputes.

The system workflow is as follows:

(1) During the registration stage, data providers and data requestors generate their fuzzy vaults for authentication with an RA.

(2) During the login stage, a user submits his face features to the AA. If his features are enough to recover the private polynomial from the vault, he passes the authentication.

(3) During the data upload stage, a student submits his answer sheet to the EP. The EP stores the ciphertext of answer sheets in a DSS and stores the pieces of evidence on the blockchain. A teacher submits the scores in a similar way.

(4) During the data request stage, a user sends a request and downloads the ciphertext from a DSS through the EP. When his attribute meets the decryption policy, the plaintext is obtained.

(5) When a dispute arises, the EA makes a judgment based on the data in a DSS and the pieces of evidence in the blockchain.

3.2. Security Model. Security threats may come from two aspects: internal and external attacks. External attacks include eavesdropping, forgery, and replay. For internal attacks, data providers may tamper with previously submitted data; data requestors may be interested in data beyond their access rights. An EP may modify some data due to the self-interest, equipment failure, and management problems. Biometric templates in an AA may leak, and the attacker may recover face images from the templates.

3.3. Design Objectives

(1) Access control: the test paper submitted by a teacher can be accessed by his students during a given time. The answer sheets submitted by students can be viewed by their relevant teachers. The test scores submitted by the teachers can be accessed by students, teachers, and an EA. Data providers can specify access policies when they generate ciphertext, and the users who satisfy the access policies can access the data.

(2) Tamper resistance: tamper resistance is very important for online examination systems. Any entity in the system cannot modify the previous uploaded data. Otherwise, it will directly affect the fairness of education.

(3) Avoidance of single-point failure: if the attribute keys are issued by one authority, the single authority easily becomes the bottleneck of the whole system. In many practical applications, data sharing is across different organizations. Attribute keys are issued by multiple authorities from different domains, which

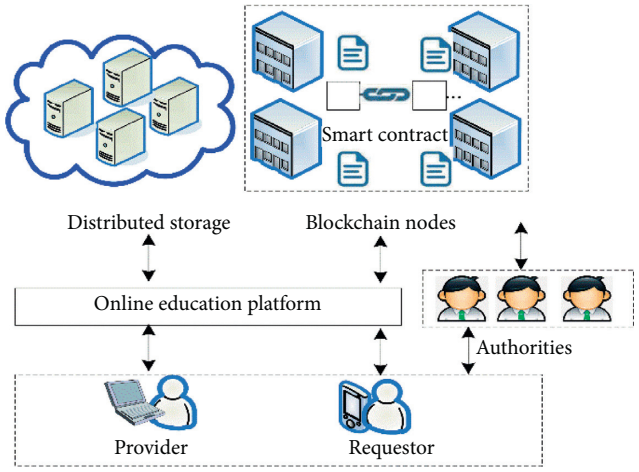

Figure 2: System framework.

Table 1: Notation.

Notation	Description
G, G_T, g	q-order groups G, G_T, generator of G
e, H	Bilinear pairing, hash function
PK, SK	Public key and private key of KA
Pubk. Prik	Public key and private key of a user
$k_{i,\text{Pubk}}$	Attribute i key of the user with Pubk
A, ρ	Access matrix and attribute function
W	Eigenfaces space
k	Feature polynomial of degree $k-1$
t	Number of principal components
V, r	Fuzzy vault and its size
Key, K	Authentication key and encryption key
CT_1	Ciphertext of data
CT_2	Ciphertext of encryption key
T_x, t_s	Proof of online examination data and timestamp

can avoid the problem of single point of failure and improve system security.

(4) Collusion resistance: when a single key is not sufficient for decryption, two or more persons try to combine their own keys for unauthorized decryption. The system requires that the combined keys cannot decrypt the correct plaintext.

(5) The determination of disputed issues: impersonating student to answer the sheet or impersonating a teacher to correct examination sheets should be found and prevented. For example, when an answer sheet is tempered, does the tampering come from an external intruder, a student, or an EP?

4. Description of the SEBB Scheme

The SEBB is built upon fuzzy vault [27, 28] and attribute encryption [29]. It consists of the following phases: system initialization, user registration, blockchain establishment, user login, data upload, data request, and dispute determination. During the registration phase, a person's facial features are encapsulated in a fuzzy vault. During the login phase, the facial features are matched with the vault data. If there are enough approximate elements, the authentication is passed; otherwise, the authentication fails. During data upload and request phases, attribute encryption and symmetric encryption are used, and data requestors with legal access rights can obtain the corresponding data.

4.1. System Initialization. During the initialization, two multiplicative cyclic groups G and G_T with the same prime order N and a map e: $G \times G \longrightarrow G_T$ are chosen. Assume g is the generator of G. A hash function H: $\{0,1\}^* \longrightarrow G$ mapping the global identities to the elements of G is provided. Assume H is a random oracle. So the global parameter $GP = \{G, G_T, N, g, e, H\}$. Then, for each attribute i belonging to one authority, the authority chooses two random exponents α_i, y_i, computes a public key $\text{PK} = \{e(g,g)^{\alpha_i}, g^{y_i}, \forall i\}$, and keeps $\text{SK} = \{\alpha_i, y_i, \forall i\}$ as its secret key.

4.2. Blockchain Establishment and Maintenance. In the blockchain, each block is generated through a consensus mechanism and contains a certain number of transactions. Due to the different access mechanism, blockchains can be divided into three categories: public blockchain, alliance blockchain, and private blockchain.

We use alliance blockchain which are constructed and maintained by several entities with high credibility. Unlike public blockchain, each node in alliance chain is usually an organization who can join the network only after authorization. A leader is chosen according to the proof-of-stake mechanism. He is responsible for creating new blocks and broadcasting them in the blockchain network.

4.3. User Registration. By executing the registration protocol, a fuzzy vault for authentication is generated, and each user gets his vault (Figure 3). In the process, n independent data items replace n-dimensional vectors, and dimension information is lost. To preserve vector information, we add dimension information to each point, that is, (x, y) is extended to (d, x, y). So, similar points are matched in the same dimension.

Suppose there are b persons registered to the RA, each person has collected c face images, and the size of each image is s. The total number of images is $M = b * c$. The RA runs feature space generation algorithm (Algorithm 1) and outputs W_{s*t}, where t is the number of feature points. A user obtains W_{s*t} from the RA. SHA, as a pseudo-random function, has anticollision property. Based on SHA, we construct a truncated hash (thash) algorithm (Algorithm 2). The output has good anticollision characteristics from the original 20 bytes to 4 bytes. Then, a fuzzy vault is generated as follows:

(1) A user executes Algorithm 3 and obtains privacy polynomial $f(x)$ of degree $k-1$.

(2) The user calculates his facial feature.

$$a = W^T * I. \tag{1}$$

Here, I is the vector corresponding to his face.

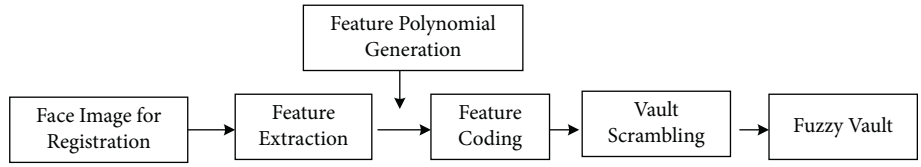

Figure 3: Facial fuzzy vault generation.

(3) He calculates the feature coding $(i, a_i, f(a_i))_{1\le i\le t}$, where a_i is the ith dimension feature of a.

(4) He randomly generates $r-t$ chaff points $(j\%t+1, x_j, y_j)_{1\le j\le r-t}$, which satisfy

$$\{(i,a_i)\}_{1\le i\le t}\cap\left\{\left(j\%t+1,x_j\right)\right\}_{1\le j\le r-t}=\varnothing,\quad y_j\neq f\left(x_j\right). \tag{2}$$

Here, r is the fuzzy vault size.

(5) He scrambles the r points and then obtains the fuzzy vault.

$$V=\left\{(d,x_m,y_m)_{1\le d\le t,1\le m\le r}\right\}, \tag{3}$$

where x_m is the dth dimension feature of the face space. He sends V to the AA.

Besides the vault V, each user needs to obtain a private key Prik and a corresponding public key Pubk from PKI. Then, Pubk is as his global identity and his blockchain account address. The user also needs to apply for the attribute keys from the KAs. If he can apply for the key of the attribute i, the KA, responsible for attribute i, computes

$$k_{i,\mathrm{Pubk}}=g^{\alpha_i}H(\mathrm{Pubk})^{y_i}, \tag{4}$$

and issues it to the user.

4.4. User Login. The authentication process is shown in Figure 4. And user login protocol is as follows:

(1) First, the user calculates his feature vector $b=W^T*I'$ and sends it to the AA, where I' is the feature vector.

(2) The AA lets userID = [ ].

(3) For each vault with different ID,

(3.1) The AA calculates the approximate intersection set.

$$Q=\{(d,b_i)\}_{1\le d\le t,1\le i\le t}\cap\left\{\left(d,x_j\right)\right\}_{1\le d\le t,1\le j\le r}. \tag{5}$$

Here, b_i is the feature points for login, and $\{x_j\}_{1\le j\le r}$ is the points in V. b_i and x_j on the same d-dimension plane are very close, satisfying $|b_i-x_j|<w$; where w is the size of the comparison window.

(3.2) If $|Q|\ge k$, call Algorithm 4 to check the validity of $f(x)$. If Algorithm 4 returns True, userID = userID + ID. Here, ID is bounded with $f(x)$.

(4) If userID is a single ID, return userID;

Else call Algorithm 5.

Our scheme shuffles the n-dimensional vector into n independent points. The distance-based comparison in traditional recognition scheme cannot be used here. The comparison based on approximate points might increase false rate. To deal with the problem, the above process adopts the idea of majority voting, which reduces false rate. In the case of returning multiple ID, the ID with the most occurrences is the final result. It takes into the situations that may be controversial.

4.5. Data Upload. If a teacher uploads test paper or a student uploads his answer sheet, he will perform the following steps.

(1) He chooses a random number K, uses symmetric encryption algorithm E to encrypt the data, and gets the ciphertext.

$$\mathrm{CT}_1=E_K(\mathrm{data}). \tag{6}$$

(2) He chooses $n\times l$ access structure matrix A, whose rows are mapped to the attributes through a function ρ. Here, n and l are attributes' number and threshold, respectively. He chooses a random $s\in Z_N$ and a random vector $v\in Z_N^l$ with s as its first entry of v. Let $\lambda_x=A_x\cdot v$, where A_x is the row x of A. It also chooses a random vector $w\in Z_N^l$ with 0 as its first entry. And let $w_x=A_x\cdot w$. Then, he chooses a random $r_x\in Z_N$. The ciphertext is computed as

$$\begin{aligned}\mathrm{CT}_2&=\left\{A,\rho,C_0,C_{1,x},C_{2,x},C_{3,x}\right\},\\ C_0&=Ke(g,g)^s,\\ C_{1,x}&=e(g,g)^{\lambda_x}e(g,g)^{\alpha_{\rho(x)}r_x},\\ C_{2,x}&=g^{r_x},\\ C_{3,x}&=g^{y_{\rho(x)}r_x}g^{w_x}.\end{aligned} \tag{7}$$

And he generates

$$\mathrm{CS}=t_s\|\mathrm{Pubk}\|\mathrm{CT}_1\|\mathrm{CT}_2\|\sigma', \tag{8}$$

where t_s is the time stamp and σ' is his signature with Prik to the previous items in CS.

(3) He calculates the transaction.

$$T_x=\left\{t_s\|\mathrm{Pubk}\|H\left(\mathrm{CT}_1\right)\|\sigma\right\}. \tag{9}$$

Input: M face images.
Output: Feature space W_{s*t}.
(1) Read face images into the matrix ϕ_{s*M}.
(2) Computing the difference images $\phi = \phi - \overline{\phi}$ by column.
(3) Calculate $C = \phi^T * \phi$.
(4) Calculate the eigenvalues $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_M > 0$ and the eigenvectors $u_1, u_2, \ldots, u_M$ of C.
(5) Search t ($t \leq M$) principal components satisfying the cumulative contribution rate $\alpha_t = \sum_{k=1}^{t} \lambda_k / \sum_{k=1}^{M} \lambda_k$ above 95%.
(6) Output feature space $W = \phi * (u_1, u_2, ..., u_t)$.

Algorithm 1: Facial feature space generation.

Input: a message m.
Output: truncated hash value thash (m).
(1) $h = \text{SHA}(m)$.
(2) $d = h[0]$ and $0Xf$.
(3) $v = [h[d], h[d+1], h[d+2], h[d+3]]$.
(4) Output v.

Algorithm 2: Truncated hash.

Input: k.
Output: polynomial $f(x)$ of degree $k-1$.
(1) Randomly generate $k-1$ integers $c_1, c_2, \ldots, c_{k-1}$.
(2) $m = c_1 \| c_2 | \ldots \| c_{k-1}$.
(3) $c_0 = \text{thash}(m)$ using Algorithm 2.
(4)) $f(x) = c_0 + c_1 x + \cdots + c_{k-1} x^{k-1}$.
(5) Output $f(x)$.

Algorithm 3: Feature polynomial generation.

Here, σ is his signature to the previous items in T_x.

(4) Through the EP, the data provider stores CS in a DSS and puts T_x into the blockchain using smart contract.

4.6. Data Request. If the teacher downloads answer sheets or the student wants to view his score, as a data requester, he will perform the following steps:

(1) A data requester sends t_s||Pubk to the EP. The EP returns the corresponding CS to the DSS.

(2) The data requester checks the signature in CS. If it is correct, he decrypts K from $\text{CT}_2 = \{A, \rho, C_0, C_{1,x}, C_{2,x}, C_{3,x}\}$. If he has the secret keys $k_{i,\text{Pubk}}$ for the rows A_x satisfying that $(1, 0, \ldots, 0)$ is in the span of these rows, he proceeds. For each x, he computes:

$$D_x = C_{1,x} \cdot \frac{e\left(H(\text{Pubk}), C_{3,x}\right)}{e\left(k_{\rho(x),\text{Pubk}}, C_{2,x}\right)}. \tag{10}$$

He then chooses some constants $c_x \in Z_N$ such that $\sum c_x A_x = (1, 0, \ldots, 0)$ and computes

$$K = \frac{C_0}{\prod_x D_x^{c_x}}. \tag{11}$$

(3) He uses K to decrypt data from CT_1, that is,

$$\text{data} = D_K\left(\text{CT}_1\right). \tag{12}$$

4.7. Dispute Determination. When there are some disputes, EA can make some judgments based on the data collected. For example, when a student questions his scores, he initiates an appeal.

(1) The student sends t_s||Pubk to the EA.

(2) Then, EA sends t_s||Pubk to the DSS and to the blockchain network. The DSS returns CS and blockchain network returns T_x.

(3) If the signature in CS or the signature in T_x is incorrect, it may be that the EP tampers with the data or an interface of the EP is intruded.

(4) If the two signatures are correct, the following cases are possible. (i) When the calculated hash value of

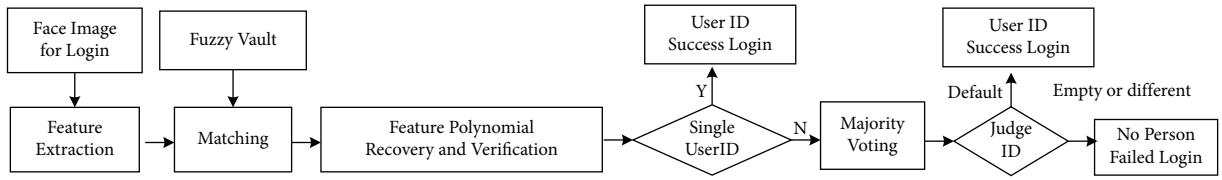

Figure 4: Biometric matching and authentication.

Input: approximate intersection set Q.
Output: True or False.
(1) Based on Q, using the Lagrange interpolation, recover the $f(x)$ with the coefficients $c_0, c_1, c_2, \ldots, c_{k-1}$.
(2) $m = c_1 \| c_2 | \ldots \| c_{k-1}$.
(3) $v = \text{thash}(m)$ using Algorithm 2.
(4) If $v = c_0$, return True.
(5) Else False.

Algorithm 4: Feature polynomial recovery and verification.

(1) Repeat twice again from Step 1 to 3 in user login protocol.
(2) Switch (userID) {
(3) Case empty:
(4) return no person;
(5) Case different ID:
(6) return no person;
(7) Default:
(8) return the ID with the most occurrences;
}

Algorithm 5: Majority voting.

CT_1 in a DSS is different from $H(CT_1)$ in the blockchain, it indicates that the data in the DSS are tempered. The tampering is caused by the data provider. (ii) The calculated hash value of CT_1 and $H(CT_1)$ are the same. But, there are two transactions in the blockchain with different timestamps for the same user in the same course examination, which indicates that the user provider submits repeatedly. In the examination, if the answer sheet is submitted twice, it may be that the student has found a better answer and replaced the original one, which is not allowed. If there is no platform cooperation, the user cannot submit twice. So, it is likely the result of collusion between the student and the EP.

5. Security Analysis

Proposition 1. *Security level for authentication increases with the increase of the vault size and the threshold value.*

An attacker guesses at least k correct features from the r points in V, and he can pass the authentication. Define r as the vault size, t as the feature number, and k as the threshold value. Only if an attacker takes t points out of r points and at least k ($k < t$) points are effective, can the coefficients of the $k-1$ degree polynomial be obtained. Figure 5 shows vulnerability analysis of authentication system. The relevant parameters are as follows:

In Figure 5(a), $r \in [450, 550]$, $t = 30$, $k = 16$;

In Figure 5(b), $t \in [25, 34]$, $r = 500$, $k = 16$;

In Figure 5(c), $k \in [11, 20]$, $r = 500$, $t = 30$.

It can be seen that the probability of successful attack decreases as the vault size increases (Figure 5(a)); with the increase of biometric features to be provided, the probability increases (Figure 5(b)); with the increase of threshold value, the probability decreases (Figure 5(c)). It means that authentication is more secure as the vault size and the threshold value increase. But when the features increase and

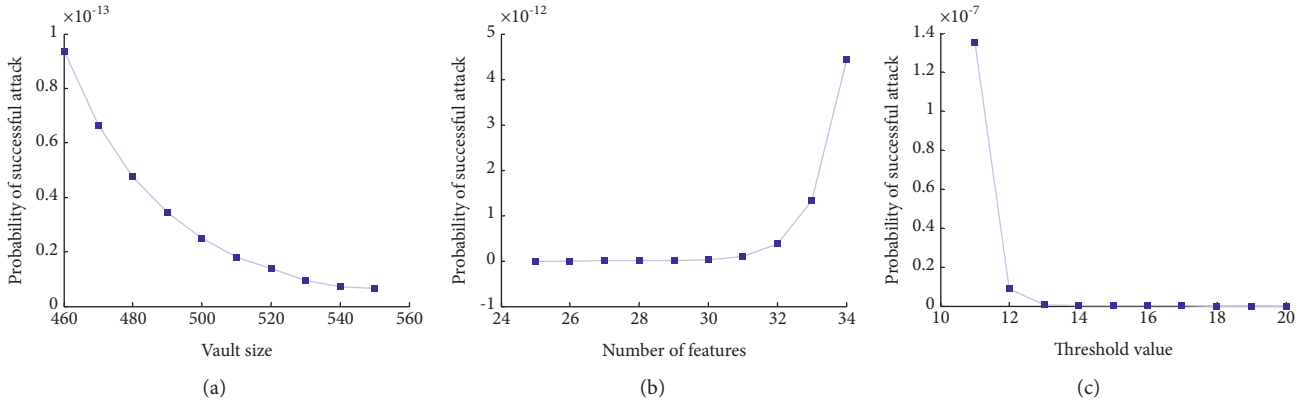

FIGURE 5: Probability of successful attack in face authentication for different (a) vault size, (b) number of features, and (c) threshold value.

other parameters remain unchanged, security will be lower because guessing the valid points is relatively easy. But, as can be seen from the figure, the probability of successful attack is still very small, that is, less than $5 * 10^{-12}$.

Proposition 2. *Even if an AA compromises, biometrics features of each user will not be leaked.*

There are r points in the vault and t effective biometric points. If the vault data are leaked, the attackers infer effective points set from V with the probability of $1/C_r^t$. When $r = 500$ and $t = 30$, the probability is $6.9192 * 10^{-49}$. It is very small and negligible.

Proposition 3. *The decryption of K from $CT_2 = \{A, \rho, C_0, C_{1,x}, C_{2,x}, C_{3,x}\}$ is correct.*

Proof 1. From the data upload and request phases, we can see

$$D_x = C_{1,x} \cdot \frac{e\left(H(\text{Pubk}), C_{3,x}\right)}{e\left(k_{\rho(x),\text{GID}}, C_{2,x}\right)} = \frac{e(g,g)^{\lambda_x} e(g,g)^{\alpha_{\rho(x)} r_x} \cdot e\left(H(\text{Pubk}), g^{y_{\rho(x)} r_x} g^{w_x}\right)}{e\left(g^{\alpha_{\rho(x)}} H(\text{Pubk})^{y_{\rho(x)}}, g^{r_x}\right)}$$

$$= \frac{e(g,g)^{\lambda_x} e\left(H(\text{Pubk}), g^{w_x}\right) e\left(g^{\alpha_{\rho(x)}}, g^{r_x}\right) \cdot e\left(H(\text{Pubk})^{y_{\rho(x)}}, g^{r_x}\right)}{e\left(g^{\alpha_{\rho(x)}} H(\text{Pubk})^{y_{\rho(x)}}, g^{r_x}\right)} = e(g,g)^{\lambda_x} e\left(H(\text{Pubk}), g\right)^{w_x},$$

$$\frac{C_0}{\prod_x D_x^{c_x}} = \frac{Ke(g,g)^s}{\prod_x \left(e(g,g)^{\lambda_x} e\left(H(\text{Pubk}), g\right)^{w_x}\right)^{c_x}} = \frac{Ke(g,g)^s}{e(g,g)^{\sum_x c_x \lambda_x} e\left(H(\text{Pubk}), g\right)^{\sum_x c_x w_x}}$$

$$= \frac{Ke(g,g)^s}{e(g,g)^{\sum_x c_x A_x v} e\left(H(\text{Pubk}), g\right)^{\sum_x c_x A_x w}} = \frac{Ke(g,g)^s}{e(g,g)^s e\left(H(\text{Pubk}), g\right)^0} = K. \tag{13}$$

□

Proposition 4. *Any entity in the system cannot modify the uploaded data. The scheme resists tamper attacks.*

Proof. The blockchain ledger has integrity, which ensures that the evidence $T_x = \{t_s \| \text{Pubk} \| H(\text{CT}_1) \| \sigma\}$ of the uploaded ciphertext CT_1 is stored in a secure and tamper-resistant manner. Once CT_1 in a DSS is tempered, it will be discovered by checking its evidence in the blockchain. □

Proposition 5. *Only the user whose attributes match the access structure, can he obtain the corresponding data.*

Proof. The KA issues attribute keys $k_{\rho(i),\text{Pubk}}$ for teachers and students. A data provider specifies the access policy (A, ρ) and writes the policy into the ciphertext using attribute encryption. The method ensures that the requestor who matches the attribute policy can calculate D_x, open $K = C_0 / \prod_x D_x^{c_x}$ and obtain data $= D_K(\text{CT}_1)$. □

Proposition 6. *Attribute keys can be issued by different KAs. The scheme avoids single-point failures.*

Proof. From the system initialization phase, we can see that different KAs need not be aware of each other, the different attribute keys belong to the same user with the help of the global identity Pubk. As the compromised KAs do not affect the work of normal KAs, the scheme can avoid a single-point failure. □

Table 2: Security features comparisons.

	Authentication	Confidentiality	Tamper proof	Avoidance of single-point failure	Dispute resolution
[10]	No	No	Yes	Yes	No
[11]	No	No	Yes	Yes	No
[19]	Yes	No	No	No	No
[22]	Yes	Yes	Yes	No	No
[23]	Yes	Yes	No	No	No
[24]	No	Yes	Yes	Yes	No
[25]	Yes	Yes	Yes	Yes	No
Our scheme	Yes	Yes	Yes	Yes	Yes

Proposition 7. *The encrypted data cannot be opened even under collusion attacks from the requestors who hold partial keys.*

Proof. A hash function on the global identity Pubk is used to resist collusion attack. Collusion attackers can obtain their own $D_x = e(g, g)^{\lambda_x} e(H(\text{Pubk}), g)^{w_x}$. Due to different Pubk, the pairing operation $e(H(\text{Pubk}), g)$ cannot be merged. So K is not obtained by calculating $C_0/\prod_x D_x^{c_x}$, and the collusion will fail. □

Proposition 8. *When the disputes arise among students, teachers, and the EP, the scheme can determine the real initiator of malicious behavior.*

Proof. According to the data consistency between the blockchain and a DSS, the tampering behavior can be judged. If the signature in the DSS or the signature in blockchain is incorrect, the tampering is caused by the EP or an interface of the EP. Otherwise, it might be caused by data provider. In particular, if there are two transactions about the same examination and the same user with different timestamps, it is a fraudulent act of repeated submission, likely caused by the collusion between the user and the EP.

We compare our scheme with existing works regarding security features in Table 2. From Table 2, it can be seen that Fenu et al. [19] focus on the authentication and it do not discuss the biometric features protection. Rashid et al. and Palma et al. [10, 11] provide tamper proof. In Kausar et al.'s study [22], a trusted server (TS) needs to use public key cryptography to distribute session keys to different users; when the number of users is large, the computational and communication overheads are very large; the system assumes that the TS is a trusted center, so a single point of failure cannot be avoided; when a dispute arises among teachers, students, and an education platform, the authority cannot make a reasonable decision. Al-Hawari et al. [23] designed an integrated and secure web-based examination management system, where the communication with authentication and confidentiality was provided. Jose and Christophe [24] proposed a secure cloud data storage approach in e-learning systems, which can resist tampering attacks and avoid single point of failure. Rahman et al. [25] designed and implemented a system with blockchain framework, data sending-receiving, and confidentiality-integrity-availability; it has higher security. However, the aforementioned works did not discuss how to resolve some disputes among students, teachers, and a platform in a fair and reasonable way. Security analysis shows that our scheme is superior to the existing schemes in terms of privacy-preserving biometric templates, fine-grained access, and dispute resolution. □

6. Performance Analysis

For convenience to evaluate the computation costs of the scheme, we ignore some operations such as a hash function and a multiplication operation because they are quite light in terms of load. As AES algorithm requires 94 μs to perform encryption with packet size of 1024 bytes, the same with decryption [30], we also ignore its execution time. Then we focused on some time-consuming operations: a bilinear map operation and an exponentiation operation. Under $|q| = 20$ bytes, it requires 4.5 ms and 0.6 ms to perform a bilinear map and a scalar multiplication, respectively, on an Intel Pentium 4 processor with the clock speed of 3.4 GHz [31]. In our scheme, we assume that $|q| = 20$ B, $|\text{data}| = 1024 * 1024$ B, the fuzzy vault size $r = 500$, the principal components number $t = 30$, the timestamp $|ts| = 2$ B, the polynomial of degree 15, the number of attributes $n = 30$, and the threshold of attributes $l = 3$.

Figures 6 and 7 show computation and communication costs during different phases, respectively. We observe that registration requires more computation and communication costs due to the generation and transmission of the vault. First, 30 feature points are embedded into the polynomial of degree 15; then, to make the vault secure, a lot of chaff points are added, and the original 30 feature points are expanded to 500 points. During the login stage, Lagrange interpolation is used to calculate polynomial coefficients without the exponential and pairing operations and the communication cost 120 B because of 30 feature points. Assuming that the data submitted have $1024 * 1024$ B, the length of uploaded message, query message, and dispute resolution message have 1,049,084 B, 1,049,011 B, and 1,049,115 B, respectively. Except the actual examine data, the length of the remaining part for upload, request, and dispute are 508 B, 435 B, and 539 B, respectively.

For other related works, Kausar et al.'s model [22] provides confidentiality and integrity. In Kausar et al.'s model [22], the server is assumed to a trusted center and distributes the session key for a specified time period, such as a class, seminar, or exam. Kausar et al.'s architecture [22] is different from ours. Based on blockchain technology, Rashid

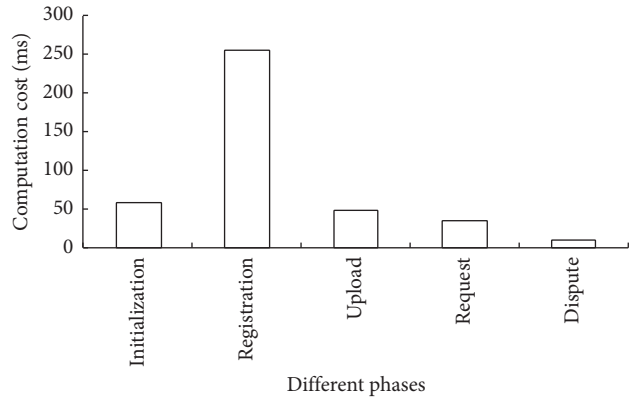

Figure 6: The computation cost comparisons in different phases.

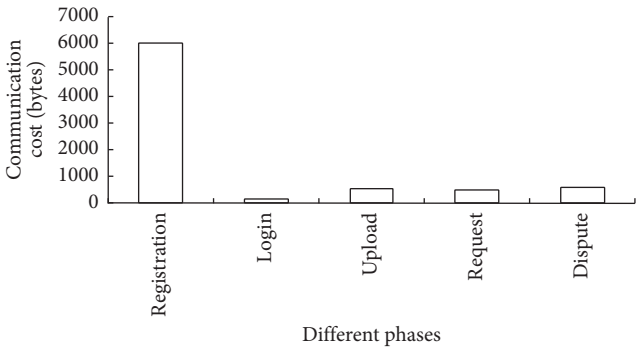

Figure 7: The communication cost comparisons in different phases (except the exam data during upload and request).

et al. [10] proposed a platform for funding needy students for their tertiary education; Palma et al. [11] presented a proposal for the digitization of degree certificates and academic credits in the Brazilian education system. In Rashid et al.'s and Palma et al.'s studies [10, 11], tamper proof is considered, but there are no more security properties and its implementation process.

Our scheme maintains better communication and computation performance during login, upload, request, and dispute phases, while providing higher security level, especially in the aspect of privacy-preserving biometric features, fine-grained access control, and avoidance of single-point failure and dispute resolution.

7. Conclusion and Future Work

Based on blockchain with openness, unforgeability, and decentralization, we propose a secure online examination scheme. In the SEBB, the institutions with high credibility jointly establish a blockchain network to record the evidence of uploaded data. The corresponding ciphertext data are stored in a DSS. Any entity cannot tamper with the uploaded data. Only the users, whose attributes match the access structure, can obtain the corresponding data. The scheme does not require any central authority, avoids single point of failure, and resists tamper attack.

For future research, we will study multibiometric systems. We plan to incorporate behavioral features (e.g., keystroke patterns) with physiological biometrics to prove that the authenticated user is the person performing teaching and learning activities.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

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

Acknowledgments

This work was supported by the Natural Science Key Research Project in Colleges and Universities of Anhui Province (grant no. KJ2019A1205) and by the Quality Engineering Project of Anhui Colleges and Universities (grant no. 2020xsxxkc351).

References

[1] E.-S. H. Farouk, T. A. Al, K. Alghatani et al., "The impact of cloud computing technologies in E-learning," *International Journal of Emerging Technologies in Learning (iJET)*, vol. 8, pp. 37–43, 2013.

[2] R. Kashyap, "Biometric authentication techniques and E-learning," *Biometric Authentication in Online Learning Environments*, IGI Global, Hershey, PA, USA, 2019.

[3] Y. Chen and W. He, "Security risks and protection in online learning: a survey," *International Review of Research in Open and Distance Learning*, vol. 14, no. 5, pp. 108–127, 2013.

[4] A. Ullah, H. Xiao, M. Lilley, and T. Barker, "Privacy and usability of image and text based challenge questions authentication in online examination," in *Proceedings of the International Conference on Education Technologies and Computers*, pp. 24–29, Lodz, Poland, September 2014.

[5] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: a technical survey on decentralized digital currencies," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 2084–2123, 2016.

[6] E. Gaetani, L. Aniello, R. Baldoni et al., "Blockchain-based database to ensure data Integrity in cloud computing environments," in *Proceedings of the First Italian Conference on Cybersecurity (ITASEC17)*, pp. 146–155, Venice, Italy, January 2017.

[7] P. Treleaven, R. Gendal Brown, and D. Yang, "Blockchain technology in finance," *Computer*, vol. 50, no. 9, pp. 14–17, 2017.

[8] D. Mills, K. Wang, B. Malone et al., "Distributed ledger technology in payments, clearing, and settlement," *Finance and Economics Discussion Series*, vol. 2016, no. 95, 2016.

[9] T. Xu, "Research on the development and significance of blockchain + education," *Journal of Distance Education*, vol. 35, no. 2, pp. 19–28, 2017.

[10] M. A. Rashid, K. Deo, D. Prasad et al., "TEduChain: a blockchain-based platform for crowdfunding tertiary education," *The Knowledge Engineering Review*, vol. 35, 2020.

[11] L. M. Palma, M. A. Vigil, A. G. Martín, F. L. Pereira et al., "Blockchain and smart contr acts for higher education registry

in Brazil," *International Journal of Network Management*, vol. 26, 2019.

[12] O. S. Saleh, O. Ghazali, and M. E. Rana, "Blockchain based framework for educational certificates verification," *Journal of Critical Reviews*, vol. 7, no. 3, pp. 79–84, 2020.

[13] A. Mikroyannidis, J. Domingue, M. Bachler et al., "A learner-centred approach for lifelong learning powered by the blockchain," in *Proceedings of the EdMedia + Innovate Learning*, Amsterdam, The Netherlands, June 2018.

[14] D. V. Kotwal, S. R. Bhadke, A. S. Gunjal et al., "Online examination system," *International Research Journal of Engineering and Technology (IRJET)*, vol. 3, no. 1, pp. 115–117, 2016.

[15] A. Okada, D. Whitelock, W. Holmes et al., "E-authentication for online assessment: a mixed-method study," *British Journal of Educational Technology*, vol. 50, no. 2, pp. 861–875, 2019.

[16] Y. Atoum, L. Chen, A. X. Liu, S. D. Hsu, and X. Liu, "Automated online exam proctoring," *IEEE Transactions on Multimedia*, vol. 99, 2016.

[17] S. Asha and C. Chellappan, "Authentication of e-learners using multimodal biometric technology," in *Proceedings of the International Symposium on Biometrics and Security Technologies*, pp. 1–6, Isalambad, Pakistan, April 2008.

[18] E. G. Agulla, E. A. Rúa, J. L. A. Castro, D. G. Jiménez, and L. A. Rifón, "Multimodal biometrics-based student attendance measurement in learning management systems," in *Proceedings of the 11th IEEE International Symposium on Multimedia (ISM)*, pp. 699–704, San Diego, CA, USA, December 2009.

[19] G. Fenu, M. Marras, and L. Boratto, "A multi-biometric system for continuous student authentication in e-learning platforms," *Pattern Recognition Letters*, vol. 113, no. 1, pp. 83–92, 2017.

[20] S. M. Al-Saleem and U. Hanif, "Security considerations and recommendations in computer-based testing," *Science World Journal*, vol. 2014, Article ID 562787, 7 pages, 2014.

[21] K. Kaczmarek, E. Chen, and H. Ohyama, "Eye in the sky: student perceptions of secure remote examinations," *Journal of Dental Education*, pp. 1–3, 2021.

[22] S. Kausar, X. Huahu, A. Ullah et al., "Fog-assisted secure data exchange for examination and testing in E-learning System," *Mobile Networks and Applications*, pp. 1–17, 2020.

[23] F. Al-HawariM. Alshawabkeh et al., "Integrated and secure web-based examination management system," *Computer Applications in Engineering Education*, pp. 994–1014, 2019.

[24] G. Sahaya Stalin Jose and C. Seldev Christophe, "Secure cloud data storage approach in e-learning systems," *Cluster Computing*, vol. 22, pp. S12857–S12862, 2019.

[25] M. A. Rahman, M. S. Abuludin, L. X. Yuan et al., "EduChain: CIA-compliant block-chain for intelligent cyber defense of microservices in education industry 4.0," *IEEE Transactions on Industrial Informatics*, pp. 1–8, 2021.

[26] H. Deenmahomed, M. M. Didier, and R. K. Sungkur, "The future of university education: examination, transcript, and certificate system using blockchain," *Computer Applications in Engineering Education*, pp. 1–23, 2021.

[27] A. Juels, "A fuzzy vault scheme," in *Proceedings of the IEEE International Symposium on Information Theory*, Lausanne, Switzerland, July 2004.

[28] P. Shang, S. Pirbhulal, W. Wu et al., "Fuzzy vault-based biometric security method for tele-health monitoring systems," *Computers & Electrical Engineering*, vol. 71, pp. 546–557, 2018.

[29] L. Allison and W. Brent, "Decentralizing attribute-based encryption," in *Proceedings of the 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 568–588, Tallinn, Estonia, May 2011.

[30] N. W. Wang, Y. M. Huang, and W. M. Chen, "A novel secure communication scheme in vehicular ad hoc networks," *Computer Communications*, vol. 31, no. 12, pp. 2827–2837, 2008.

[31] L. Chen, S. L. Ng, and G. Wang, "Threshold anonymous announcement in VANETs," *Selected Areas in Communications*, vol. 29, no. 3, pp. 605–615, 2011.