S & M 2902

Applying Secure Access Based on Lagrange Interpolation Polynomial to Online Learning Sensor Platform

Yao-Min Huang,[1] Yu-Fang Chung,[2] Dai-Lun Chiang,[3]
Ya-Hsin Chang,[4] Tzer-Shyong Chen,[5*] and Chih-Cheng Chen[6]

[1]Department of Management Science, National Yang Ming Chiao Tung University,
No. 1001, University Road, Hsinchu 30010, Taiwan
[2]Department of Electrical Engineering, Tunghai University,
No. 1727, Sec. 4, Taiwan Blvd, Xitun District, Taichung City 407224, Taiwan
[3]Financial Technology Applications Program, Ming Chuan University,
No. 5, De Ming Rd, Gui Shan District, Taoyuan City 333, Taiwan
[4]Department of Multimedia Game Development and Application, HungKuang University,
No. 1018, Sec. 6, Taiwan Boulevard, Shalu District, Taichung City 433304, Taiwan
[5]Department of Information Management, Tunghai University,
No. 1727, Sec. 4, Taiwan Blvd, Xitun District, Taichung City 407224, Taiwan
[6]Department of Automatic Control Engineering, Feng Chia University,
No. 100, Wenhua Rd, Xitun District, Taichung City 407, Taiwan

(Received September 14, 2021; accepted February 9, 2022)

Keywords: digital resource sharing system, access control mechanism, Lagrange interpolation polynomial, key cryptography system, timestamp

We propose a cloud-based digital sensor resource sharing system and combine it with an image sensor and an access control mechanism to establish a secure environment. In recent years, the IoT has profoundly changed the model of education, with students learning on online courses via mobile phones or IoT devices without limitations of time and space. IoT makes e-learning accessible in more places and in more ways. Students can use sensing or terminal devices to interact with teaching materials on the cloud platform. Data privacy is a major concern for engaged online users. In this study, we first identify feature points, using an image sensor to confirm that a user is legitimate. Then we use a Lagrange interpolation polynomial and a key cryptography system to control the encryption and decryption of the user's login to the system, where we utilize hierarchical access control in the method. Therefore, the access control method is set to manage the data that everyone can access. Additionally, we apply a timestamp to manage the limited time in which users are allowed to access the files. The timestamp is also integrated in the system to create a complete access control structure to effectively improve the functionality of the cloud-based digital sensor platform. Identity verification is strictly used to control the user's access rights, and the exclusive settings of all users are controlled to ensure their overall rights and the security of the system. Our proposed system can also prevent both external and internal malicious attackers. A single user or a malicious group should have no opportunity to invade this system or steal or modify user data. Access control management and system compatibility have become primary issues in the access and delivery of digital material. Accordingly, we provide a more efficient method for optimizing the use of digital material such as online platforms in e-learning and enhancing the quality of digital sharing.

[*]Corresponding author: e-mail: arden@thu.edu.tw
https://doi.org/10.18494/SAM3656

1. Introduction

1.1 Research background

Portable devices have become essential items in our daily lives. Mobile phones, tablets, laptops, and other digital tools are continuously connected to the internet and the cloud. Students can overcome the limitations of time and space to access data using these devices. Although the concept of online learning is mature, it can still be improved. Protective mechanisms to prevent the theft of personal information are prioritized in online learning and will be discussed in this paper. Furthermore, infrastructures are necessary for building online learning platforms. Online learning platforms enhance the compatibility of entire systems and the development of related applications. The purpose of constructing such mechanisms is to provide information platforms for users and to increase security and confidentiality during the transfer of information.

The online working environments for users are diversified and convenient. Their features require cloud computing to be equipped with multiple functions. Cloud computing must deal with the input of massive amounts of information, with users, and with simultaneous requests from different types of devices.(1) To meet the need for information security, we have developed an improved access control mechanism in this study. Our proposed system can also access any network device connected via IoT. The system assigns different levels of access permission for different users according to their level of authority, enabling users to access files quickly, stably, and safely in a specified time.

1.2 Research motivation

The greatest advantage of online learning is the function of sharing, which allows multiple users to access a system simultaneously. Because of this function, the efficiency and security of processing systems have become major issues. The security of online learning sensor platforms has become important because of the increasing number of user devices connected to the internet. Therefore, education in IoT security has become necessary. Different access settings for different levels of authority are also essential, and the prevention of illegal users has become a priority to ensure the confidentiality of each user. Although IoT brings unprecedented convenience to users, the issue of how to control permissions and increase the security of all devices and platforms must also be addressed. To resolve these issues, we are developing online education platforms with a safe environment. The motivation of this study is to develop a protective measure to prevent systems from internal and external attack.

1.3 Research goal

Cloud resource management is a service in which all authorized suppliers can upload resources to a cloud platform after a system is built in the cloud. Our proposed system includes different kinds of users. The problems encountered by users often increase the burden of administrators. Thus, the efficiency in offering cloud resources for users might be an issue. An automated cloud service reduces the burden on the system and increases its loading efficiency. The massive amount of data both uploaded and downloaded from the cloud will increase the load of the system. By using a cloud resource monitor, administrators can control the use of resources, ensuring that the cloud and the virtual host function smoothly. The concept of centralized management includes cloud-based resource monitoring. Using a well-designed management interface, administrators can provide information whenever users encounter problems, increasing the comprehensiveness and safety of the cloud service. The growth of IoT in education has also led to an explosion of cyber security threats because the proliferation of sensors and connected devices has greatly increased the scope for network attack.

The goal of our research is to develop an access control mechanism with both safety and high efficiency. The mechanism will be incorporated in an e-learning environment containing a massive amount of data. It can provide each layer with a specific definition of access authority, making it suitable for a workspace with multiple users. Traditional cloud platforms have their own encryption technique to protect data. However, they only focus on the structure of a single owner and are not equipped with a timestamp to improve security. In addition, previously developed protective measures may not be effective or safe in a cloud system with a large number of users and a complicated working environment. To overcome the limitations of traditional protective mechanisms, we propose a new mechanism that is suitable for ensuring the security of current e-learning systems and can meet future challenges. By reducing the complexity of security management, the new mechanism can satisfy simultaneous access requests from different users. In addition, by adding a timestamp, it can ensure secure access for a period of validity, thus resolving the difficulties of authorizing and controlling digital resource access in the cloud. Furthermore, we also use an image sensor to identify a characteristic value to confirm that a user is legitimate.

2. Literature Review

Copyright protection of digital resources is the most important issue in cloud-based sharing, where mandatory access control (MAC), discretionary access control (DAC), and role-based access control are examples of access control mechanisms. MAC is based on manager authorization, allowing users to access all information components authorized by managers.(2) DAC is based on authorization by the information component holder, giving users the right to access information components without manager authorization.(3) In role-based access control, access rights depend on the user role, and users are authorized to access information components immediately after acquiring their role identity.(4)

Access control is mainly used for ensuring the security of information records and host system facilities, avoiding access without authorization, and protecting the integrity of information records. The main purpose of the host system is to establish the location of a user trying to access a document when the user requests access to a document through the access control system, as well as to judge whether the user has the right to access the document. An access control matrix is used in this kind of access control.(5)

Access control is a mechanism that can manage system resources through an operating system to protect the information system and prevent unauthorized users from access. It controls the resources that each user can access. According to the right and role of the user, it can access various document records. It aims to protect information and ensure the security of the system, to protect user's utilization within their authorized right, to block anyone without the right to access and modify records, and to reduce the opportunity for attackers to steal documents or attack the system. Access control, through right-setting management, includes access control of the access control matrix and subject-oriented access control list, and role-based access control.

2.1 Image recognition

Through Ref. 6, we can discuss the features of human faces and classify facial features, which are geometrically represented by the shapes of reference points or facial blocks.(7) We can analyze facial contours with technology that detects facial movements and extract all facial features with key points technology.(8) These technologies have a high recognition rate of about 85%.

2.2 MAC

MAC restricts users' access to files and regulates their use through mandatory regulations, thereby restricting their access behavior.(9) The setting of authority ownership adopts centralized management. Access permissions must be set through unified management of the system. The system classifies all users and document files with different security level labels. If a user attempts to access a document file, the system classifies the authorization based on the security level of the user and the file, directory, or peripheral device. Additionally, users cannot arbitrarily change their authorization basis for personal reasons. The system compares the security levels of the user and the document file. If the user level is equal to or higher than the document file level, then the user can access the document file. On the other hand, if the user level is lower than the document file level, then the user cannot obtain permission to access the document file and is blocked from reading the document by the system.(10) Security levels are a mandatory requirement, and no user or user program can be modified by another person. If the system determines that a user has a certain security level, then it is not appropriate for the user to access certain types of resources, and also the user has no right to authorize these resources.(2,11) Compared with a free control feature, an access authority with higher computational complexity is required. MAC is suitable for contexts with relatively high security requirements such as national defense, medical environments, and the copyright of digital teaching materials.

2.3 Lagrange interpolation polynomial

A Lagrange interpolation polynomial is a simple concept: a degree $n - 1$ polynomial that can pass through a set of n points on the x–y plane. A mathematical method can efficiently derive the polynomial only from different points on a plane. Nevertheless, the relationship between variables x and y cannot be definitely verified in many cases. In such cases, interpolation is applied to select the points in the x–y plane to acquire a Lagrange interpolation polynomial.(2)

Access control employs multiple methods, such as access control with linear pairing, to store e-learning data on an e-learning platform with numerous document records, where general traditional access control would result in intensive computation for the server.(12) Therefore, effective utilization is the key point in this study. The security of an access control system for digital teaching with dynamic access and a reduced computing load are the goals of this study.

3. Research Methodology

3.1 Research structure

In our proposed system, we utilize image recognition to identify users and prevent unauthorized data access. A timestamp is added to the dynamic access mechanism by which users access copyrighted digital resources to protect the resources. To integrate cloud security access in the dynamic access mechanism, a timestamp is utilized for each function of the cloud-based digital resource sharing system after a user has been verified through image recognition.

The aims of setting a key with a Lagrange interpolation polynomial are to validate the right of each user to read document records, allow users to transmit and revise documents, and provide reading rights to designated users.(13) A Lagrange interpolation polynomial can be used to implement such functions. In the access mechanism based on a Lagrange interpolation polynomial proposed in this study, interpolation polynomials are derived from several points. When the function variables are restrained by one or more conditions, the interpolation polynomial obtained from the coordinates of several points is optimized with n variables and k constraints into the solution of an equation with $n + k$ variables. Access control with a timestamp aims to integrate a scalar function and a hash function to set the validity of document records through the function of a timestamp.(14) In the access mechanism based on an interpolation polynomial, each secret key is generated distinctly with non-correspondences among keys. When people try to crack records without authorization, the time required would exceed the time set by the timestamp. Moreover, a user can generate a personal key to add, revise, and remove authorized records in a cloud-based digital resource sharing system as well as authorize specific users to access their digital information. The cloud system structure is shown in Fig. 1.

3.2 Method of constructing system

This section covers the system's setup and construction, as well as how to establish the user identity and approve access rights among records. Furthermore, the built access control matrix is used to calculate access polynomials for users to construct decryption polynomials. In the remaining sections, we consider the security of decryption polynomials in the operation of users' dynamic access mechanisms, which include adding, removing, and updating records within a given time frame. The parameters used in this research are shown in Table 1. The following steps describe the method of how we construct this system.

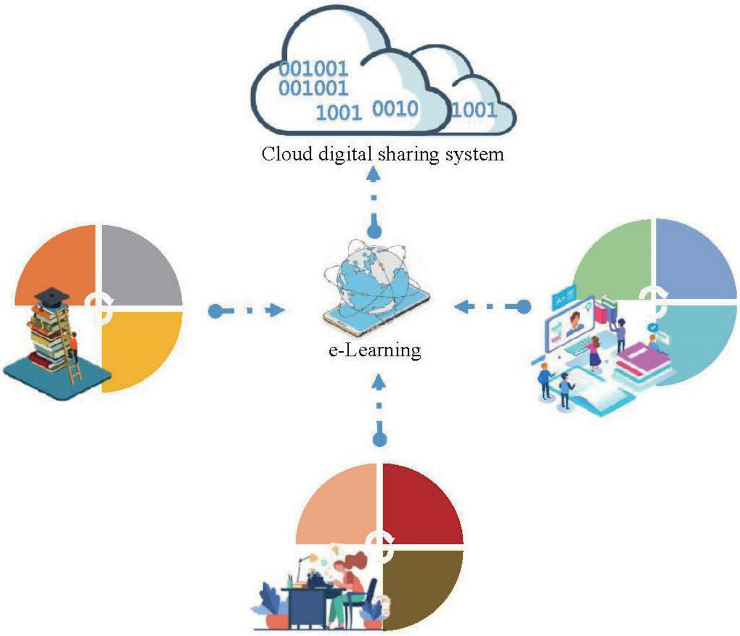

Fig. 1. (Color online) Application fields of cloud security access control.

Table 1
Notation table.

Notation	Definition
S_i	ith user
H_i	ith user's private key
DK_u	decryption key
$file_u$	document records
u	records index for users with authorized access
$A_i(x)$	user authentication
$B_i(y)$	verification of record authorization
$\theta_i^{(r)}(x)$	indicate function
d	minimum time set
z	time constraint
p	random prime
Q	random constant
$TS(k)$	time set
k	time
m	maximum
$G^{(r)}(x,y)$	public decryption polynomial
$\overline{G^{(r)}(x,y)}$	add user polynomial
$\overline{\overline{G^{(r)}(x,y)}}$	remove user polynomial

Step 1: Establish a system user list. A partially ordered set is used to establish an access relationship in the system. (S_i, $\preccurlyeq$) stands for a partially ordered set; the symbol "$\preccurlyeq$" represents reflexivity or antisymmetry, corresponding to delivering the binary data

symbols in set S. A partial order relation is defined on a set S, where the binary relationship $\preccurlyeq$ has reflexive, antisymmetric, and transitive characteristics. Different users in set S are denoted as S_i; the record data access right is set according to each user's identity. H_i stands for a user's private key. Given sets $S = \{S_1, S_2, ..., S_n\}$ and $H = \{H_1, H_2, ..., H_n\}$, the system constructs a user list composed of n users.

Step 2: In consideration of security, an array associating users and data records is established and an access function is used in this system. First, the system encrypts the data available for user access and constructs a set $file = \{file_1, file_2, ..., file_m\}$ composed of m records. Each record $file_u$ (for $u = 1, 2, ..., m$) includes the corresponding decryption key DK_u to protect encrypted documents from being randomly accessed by internal or external users without authorization.

Step 3: When user S_i acquires the authorization of a decryption key corresponding to an encrypted record, S_i is expressed as

$$S_i = \{u\text{: } u \text{ is the record index of } S_i \text{ with authorized access}\}, \tag{1}$$

where $i = 1, 2, ..., n$ and $n \in N$. For set $(S, \preccurlyeq)$, $S_j \preccurlyeq S_i$ $(i, j \in N)$ indicates that user S_i has access to the encrypted records for which user S_j requires access authorization, although legal authorization is not acquired. For instance, $S_j \preccurlyeq S_i$ when $S_j =\{1, 2\}$ and $S_i = \{1, 2, 3\}$, $\{1, 2\} \preccurlyeq \{1, 2, 3\}$. In this case, S_i can access the encrypted records $file_1$ and $file_2$ of S_j using the decryption keys.

User access to confidential records is expressed by the establishment of an access control matrix, as shown in Fig. 2. In the matrix, value 1 stands for a user with the right to access records, and value 0 represents no right. According to the access control matrix in Fig. 2, user S_2 is authorized to access $file_1$, $file_2$, $file_4$, and $file_5$ but not $file_3$. Each user S_1, S_2, ..., S_5 has an exclusive private key H_1, H_2, ..., H_5, and each confidential record $file_1$, $file_2$, ..., $file_4$ has an independent decryption key DK_1, DK_2, ..., DK_4. To access a record, it is necessary to acquire its decryption key.

The indicate function $I(x, y)$ is applied to define access and judge whether a user is authorized to acquire DK_u and thus access $file_u$.

$$\begin{array}{c|ccccc|}
 & file_1 & file_2 & file_3 & file_4 & file_5 \\
S_1 & 1 & 1 & 1 & 1 & 1 \\
S_2 & 1 & 1 & 0 & 1 & 1 \\
S_3 & 1 & 0 & 0 & 1 & 0 \\
S_4 & 0 & 0 & 0 & 1 & 0 \\
S_5 & 0 & 0 & 0 & 0 & 1
\end{array}$$

Fig. 2. Access control matrix.

For the example in Fig. 2, $I(4, 4) = 1$, i.e., user S_4 with private key H_4 can acquire DK_4 to access $file_4$, and $I(4, 3) = 0$ shows that user S_4 is not authorized to acquire decryption key DK_3 for record $file_3$.

The novelty of this study lies in incorporating time constraint z in polynomials $A_i^{(r)}(x)$ and $B_i^{(r)}(y)$,

$$z = 24(x \bmod p) + TS(k), \tag{2}$$

where $TS(k)$ is the kth hour in time set TS.

Each user has an unrepeated and unique coding for the access time so that the system can perform table-structured management. The coding after the process of mod 24 denotes the decryption process used to calculate the access time for the user.

We first divide user x by random prime p, so that each person acquires an unrepeated random number, which is non-repeated, and an access interval. A random prime is used to ensure that a nonzero remainder is obtained. This remainder is then multiplied by 24 for decryption.

For example, user S_1 in Fig. 2 with the user code $x = 1$ can access the time intervals of the first, second, and third hours, denoted as $TS = \{1, 2, 3\}$, and user S_2 with the user code $x = 2$ can access time intervals of the second, third, and fourth hours, denoted as $TS = \{2, 3, 4\}$; the random prime p is separately set as 5 and 7 to acquire the indices in Table 2. The numbers 25, 26, and 27 in Table 2 mean the time that S_1 can legally access the documents; the numbers 50, 51, and 52 mean the time that S_2 can legally access the documents.

When the index is divided by 24, the time data are acquired and the index is not repeated, ensuring that a user has access at the correct time. The establishment of the access polynomial is shown below.

Step 1: On the basis of the access control matrix, a certificate authority (CA) builds new polynomials $A_i^{(r)}(x)$ and $B_i^{(r)}(y)$ for a user, where $A_i^{(r)}(x)$ authenticates the user's identity and $B_i^{(r)}(y)$ verifies whether the user can access each record.

Step 2: $A_i^{(r)}(x)$ is used to establish a Lagrange interpolation polynomial with the user's private key, where $I_{H_i}^{(r)}$ verifies whether private key H_i is in the legal list.

$$A_i^{(r)}(x) = \left\{ \prod_{1\le k\le n, k\ne i} \left[\frac{x - H_k}{H_i - H_k} + \left(x - H_i\right) \right] + d\left(z \bmod 24 - current\ hour\right)Q \right\} \times I_{H_i}^{(r)} \tag{3}$$
$$i = 1, 2, \ldots, n, x \in R$$

Table 2
Indices.

Index
25
26
27
50
51
52

$$A_1^{(r)}(x)=\left\{\left[\frac{x-H_2}{H_1-H_2}+(x-H_1)\right]\times\left[\frac{x-H_3}{H_1-H_3}+(x-H_1)\right]\times\left[\frac{x-H_4}{H_1-H_4}+(x-H_1)\right]\right.$$
$$\left.\times\left[\frac{x-H_5}{H_1-H_5}+(x-H_1)\right]+d\left(z \bmod 24-current\,hour\right)Q\right\}\times I_{H_1}^{(r)} \tag{4}$$

$$A_2^{(r)}(x)=\left\{\left[\frac{x-H_1}{H_2-H_1}+(x-H_2)\right]\times\left[\frac{x-H_3}{H_2-H_3}+(x-H_2)\right]\times\left[\frac{x-H_4}{H_2-H_4}+(x-H_2)\right]\right.$$
$$\left.\times\left[\frac{x-H_5}{H_2-H_5}+(x-H_2)\right]+d\left(z \bmod 24-current\,hour\right)Q\right\}\times I_{H_2}^{(r)} \tag{5}$$

$$A_3^{(r)}(x)=\left\{\left[\frac{x-H_1}{H_3-H_1}+(x-H_3)\right]\times\left[\frac{x-H_2}{H_3-H_2}+(x-H_3)\right]\times\left[\frac{x-H_4}{H_3-H_4}+(x-H_3)\right]\right.$$
$$\left.\times\left[\frac{x-H_5}{H_3-H_5}+(x-H_3)\right]+d\left(z \bmod 24-current\,hour\right)Q\right\}\times I_{H_3}^{(r)} \tag{6}$$

$$A_4^{(r)}(x)=\left\{\left[\frac{x-H_1}{H_4-H_1}+(x-H_4)\right]\times\left[\frac{x-H_2}{H_4-H_2}+(x-H_4)\right]\times\left[\frac{x-H_3}{H_4-H_3}+(x-H_4)\right]\right.$$
$$\left.\times\left[\frac{x-H_5}{H_4-H_5}+(x-H_4)\right]+d\left(z \bmod 24-current\,hour\right)Q\right\}\times I_{H_4}^{(r)} \tag{7}$$

$$A_5^{(r)}(x)=\left\{\left[\frac{x-H_1}{H_5-H_1}+(x-H_5)\right]\times\left[\frac{x-H_2}{H_5-H_2}+(x-H_5)\right]\times\left[\frac{x-H_3}{H_5-H_3}+(x-H_5)\right]\right.$$
$$\left.\times\left[\frac{x-H_4}{H_5-H_4}+(x-H_5)\right]+d\left(z \bmod 24-current\,hour\right)Q\right\}\times I_{H_5}^{(r)} \tag{8}$$

where $d(z) = min_{TS}||z||$.

Parameter d is used to ensure that the computed value is both the minimum time set and positive. Each user's access time interval is known from the reminder obtained following the computation using mod, which is subtracted from the access time required by the user. When this remainder satisfies the access time allowed by the system, it is set to 0 to ensure continuous computing. In contrast, when the user does not have access at a certain time, the random constant Q is multiplied to create a very large number, and the system stops computing. $I_{H_i}^{(r)}=\begin{cases}1, & \text{if } x\in\{H_i,\ldots,H_n\}\\ 0, & \text{otherwise}\end{cases}$ verifies the validity of H_i.

Step 3: It is ensured that the following functions are satisfied. When H_i is a legal secret key, $\theta_i^{(r)}(x) = 1$; otherwise, it is 0.

$$\theta_i^{(r)}(x) = I_1^{(A_i^{(r)}(x))},\ \theta_i^{(r)}(H_i) = 1, \theta_i^{(r)}(\neq H_i) = 0. \tag{9}$$

Step 4: A new secret polynomial $B_i^{(r)}(y)$ is established to allow a legal user with a legal secret key to access the record.

$$B_i^{(r)}(y) = \left[b_{m-1}^{(i)} y^{m-1} + \ldots + b_1^{(i)} y + b_0^{(i)} + d\left(x \bmod p + TS(t) - current\,time\right)Q\right] \times I_{J_i}^{(y)} y \in R. \tag{10}$$

$$B_1(y) = \begin{bmatrix} DK_1 \times \dfrac{(y-2)(y-3)(y-4)(y-5)}{(1-2)(1-3)(1-4)(1-5)} \\ +DK_2 \times \dfrac{(y-1)(y-3)(y-4)(y-5)}{(2-1)(2-3)(2-4)(2-5)} \\ +DK_3 \times \dfrac{(y-1)(y-2)(y-4)(y-5)}{(3-1)(3-2)(3-4)(3-5)} \\ +DK_4 \times \dfrac{(y-1)(y-2)(y-3)(y-5)}{(4-1)(4-2)(4-3)(4-5)} \\ +DK_5 \times \dfrac{(y-1)(y-2)(y-3)(y-4)}{(5-1)(5-2)(5-3)(5-4)} \end{bmatrix} \times I_{J_1}(y) + d\left(x \bmod p + TS(t) - current\,time\right)Q \times I_{J_1}^{(y)} \tag{11}$$

$$B_2(y) = \begin{bmatrix} DK_1 \times \dfrac{(y-2)(y-3)(y-4)(y-5)}{(1-2)(1-3)(1-4)(1-5)} \\ +DK_2 \times \dfrac{(y-1)(y-3)(y-4)(y-5)}{(2-1)(2-3)(2-4)(2-5)} \\ +DK_4 \times \dfrac{(y-1)(y-2)(y-3)(y-5)}{(4-1)(4-2)(4-3)(4-5)} \\ +DK_5 \times \dfrac{(y-1)(y-2)(y-3)(y-4)}{(5-1)(5-2)(5-3)(5-4)} \end{bmatrix} \times I_{J_2}(y) + d\left(x \bmod p + TS(t) - current\,time\right)Q \times I_{J_2}^{(y)} \tag{12}$$

$$B_3(y) = \begin{bmatrix} DK_1 \times \dfrac{(y-2)(y-3)(y-4)(y-5)}{(1-2)(1-3)(1-4)(1-5)} \\ +DK_4 \times \dfrac{(y-1)(y-2)(y-3)(y-5)}{(4-1)(4-2)(4-3)(4-5)} \end{bmatrix} \times I_{J_3}(y) + d\left(x \bmod p + TS(t) - current\,time\right)Q \times I_{J_3}^{(y)} \tag{13}$$

$$B_4(y)=\left[DK_4\times\frac{(y-1)(y-2)(y-3)(y-5)}{(4-1)(4-2)(4-3)(4-5)}\right]\times I_{J_4}(y)+d\left(x\bmod p+TS(t)-current\,time\right)Q\times I_{J_4}^{(y)} \tag{14}$$

$$B_5(y)=\left[DK_5\times\frac{(y-1)(y-2)(y-3)(y-4)}{(5-1)(5-2)(5-3)(5-4)}\right]\times I_{J_5}(y)+d\left(x\bmod p+TS(t)-current\,time\right)Q\times I_{J_5}^{(y)} \tag{15}$$

$J_i = \{u|1 \leq u \leq m, u$ is a code denoting the authorization of the ith user to access a confidential record$\}$. (16)

The set of numbers TS contains a time interval during which the user can access records. Similar to the equation for $A_i^{(r)}(x)$, the computing is not continued when the value is not 0.

In the above equations, $I_{J_i(y)}=\begin{cases}1, & \text{if } y\in J_i\\ 0, & \text{otherwise}\end{cases}$ is the function used to verify the user's authorization to access decryption key DK_u.

Step 5: Finally, the CA builds and publicizes the following decryption equation:

$$G^{(r)}(x,y)=\sum_{i=1}^{n}A_i^{(r)}(x)B_i^{(r)}(y)\wedge x,y\in R. \tag{17}$$

4. Dynamic Access Control of Users and Records

This section verifies the security of the method proposed in this study, including the authorized setup of access rights between each user and record. The access control matrix is used to calculate the user-specific access polynomials and to construct the decryption polynomials. The following subsections examine the security of the system decryption polynomials as well as the operation of user dynamic access, which includes adding and removing users in a limited time frame as well as changing records.

4.1 Security test of decryption polynomial

It is assumed that five users are authorized to access up to five confidential documents in TS = {6,7,8,9,10,11,12}. User S_4 is authorized to access records 1, 2, and 4 at a certain time, as shown in Fig. 3.

The user H_4 first substitutes polynomial $A_4^{(r)}(x)$, TS = 6:

$$\begin{array}{c|ccccc|}
 & \begin{matrix} file_1 \\ (DK_1) \end{matrix} & \begin{matrix} file_2 \\ (DK_2) \end{matrix} & \begin{matrix} file_3 \\ (DK_3) \end{matrix} & \begin{matrix} file_4 \\ (DK_4) \end{matrix} & \begin{matrix} file_5 \\ (DK_5) \end{matrix} \\
S_1(H_1) & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} \\
S_2(H_2) & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{0} \\
S_3(H_3) & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} \\
S_4(H_4) & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} \\
S_5(H_5) & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1}
\end{array}$$

Fig. 3. Access matrix of users.

$$\begin{aligned}
A_4^{(r)}(x) &= \left\{ \prod_{1\le k\le 6, k\ne 1} \left[\frac{x-H_k}{H_i-H_k} + \left(x-H_4\right) \right] + min_{TS}\ \|z \bmod 24 - current\ hour\|Q \right\} \times I^{(H_4)}_{\{H_1,\ldots,H_6\}} \\
&= \left[\frac{x-H_1}{H_4-H_1} - \left(x-H_4\right) \right] \times \left[\frac{x-H_2}{H_4-H_2} - \left(x-H_4\right) \right] \times \left[\frac{x-H_3}{H_4-H_3} - \left(x-H_4\right) \right] \\
&\quad \times \left[\frac{x-H_5}{H_4-H_5} - \left(x-H_4\right) \right] \times \left[\frac{x-H_6}{H_4-H_6} - \left(x-H_4\right) \right] \times I^{(H_4)}_{\{H_1,\ldots,H_6\}} \\
&\quad + min_{TS}\ \|z \bmod 24 - current\ hour\|Q \times I^{(H_4)}_{\{H_1,\ldots,H_6\}} \\
&= 1.
\end{aligned} \tag{18}$$

When $I^{(H_4)}_{\{H_1,\ldots,H_6\}} = 1$ and $TS = 6$, we have

$$min_{TS}\ \|z \bmod 24 - current\ hour\|Q = 0\,. \tag{19}$$

As a result, $A_4^{(r)}(x) = 1$. Similarly, the value of $\theta_i^{(r)}(x) = I_1^{(A_i^{(r)}(x))}$ is 1, and the polynomial $A_4^{(r)}(x)$ is verified to have a value of 1.

Assuming that the same user S_4 intends to access records 1, 2, and 4 in non-access time, $t \ne TS$, then $\| z \bmod 24 - current\ hour \| Q \ne 0$ is not derived from polynomial $A_4^{(r)}(x)$ and authentication is not given.

After the verification of polynomial $A_4^{(r)}(x)$ for user S_4, the authorization to access records 1, 2, and 4 is also verified when $TS = 6$; $J_4 = \{1,2,4\}$ is then substituted into $B_4^{(r)}(y)$:

$$\begin{aligned}
B_4^{(r)}(y) &= \left\{ \left[\begin{aligned} & DK_1 \times \frac{(y-2)(y-3)(y-4)(y-5)}{(1-2)(1-3)(1-4)(1-5)} \\ & + DK_2 \times \frac{(y-1)(y-3)(y-4)(y-5)}{(2-1)(2-3)(2-4)(2-5)} \\ & + DK_4 \times \frac{(y-1)(y-2)(y-3)(y-5)}{(4-1)(4-2)(4-3)(4-5)} \end{aligned} \right] + min_{TS}\ \|z \bmod 24 - current\ hour\,\|Q \right\} \times I_{J_4(y)} \\
&= DK_4
\end{aligned} \tag{20}$$

The conditions $I_{J_4}(1)=1,\ I_{J_4}(2)=1,\ I_{J_4}(4)=1,\ B_4^{(r)}(1)=DK_1,\ B_4^{(r)}(2)=DK_2,\ B_4^{(r)}(3)=0,$ $B_4^{(r)}(4)=DK_4,\ B_4^{(r)}(5)=0$ are further confirmed. Moreover, after $TS = 6$, we have

$$min_{TS}\ \|z \bmod 24 - current\ hour\| Q = 0\,. \tag{21}$$

When user S_4 intends to acquire decryption key DK_2, $A_4^{(r)}(H_4)B_4^{(r)}(2)$ is reviewed and $G^{(r)}(H_4, 2)$ is calculated as follows.

$$\begin{aligned} G^{(r)}(H_4,2) &= A_1^{(r)}(H_4)B_1^{(r)}(2) + A_2^{(r)}(H_4)B_2^{(r)}(2) + A_3^{(r)}(H_4)B_3^{(r)}(2) \\ &\quad + A_4^{(r)}(H_4)B_4^{(r)}(2) + A_5^{(r)}(H_4)B_5^{(r)}(2) + A_6^{(r)}(H_4)B_6^{(r)}(2) \end{aligned} \tag{22}$$

$$\begin{aligned} A_4^{(r)}(x) &= \left\{ \prod_{1\le k\le 6,\ k\ne 1} \left[\frac{x-H_k}{H_i-H_k} + \left(x-H_4\right) \right] \right\} \times I^{(H_4)}_{\{H_1,\ldots,\,H_6\}} \\ &= \left[\frac{x-H_1}{H_4-H_1} - \left(x-H_4\right) \right] \times \left[\frac{x-H_2}{H_4-H_2} - \left(x-H_4\right) \right] \times \left[\frac{x-H_3}{H_4-H_3} - \left(x-H_4\right) \right] \\ &\quad \times \left[\frac{x-H_5}{H_4-H_5} - \left(x-H_4\right) \right] \times \left[\frac{x-H_6}{H_4-H_6} - \left(x-H_4\right) \right] \times I^{(H_4)}_{\{H_1,\ldots,\,H_6\}} \\ &\quad + min_{TS}\ \|z \bmod 24 - current\ hour\| Q \times I^{(H_4)}_{\{H_1,\ldots,\,H_6\}} \\ &= 1 \end{aligned} \tag{23}$$

$$\begin{aligned} B_4^{(r)}(y) &= \left\{ \left[\begin{aligned} & DK_1 \times \frac{(y-2)(y-3)(y-4)(y-5)}{(1-2)(1-3)(1-4)(1-5)} \\ & +DK_2 \times \frac{(y-1)(y-3)(y-4)(y-5)}{(2-1)(2-3)(2-4)(2-5)} \\ & +DK_4 \times \frac{(y-1)(y-2)(y-3)(y-5)}{(4-1)(4-2)(4-3)(4-5)} \end{aligned} \right] + min_{TS} \|z \bmod 24 - current\ hour\| Q \right\} \times I_{J_4(y)} \\ &= DK_4 \end{aligned} \tag{24}$$

J = {1,2,5,6} means that the user has access at the first, second, fifth, and sixth hours, then $A_j^{(r)}(H_4) \ne 1$ and $B_{J4}^{(r)}(y) = 0$.

As a result,

$$\begin{aligned} G^{(r)}(H_4,2) &= A_1^{(r)}(H_4)B_1^{(r)}(2) + A_2^{(r)}(H_4)B_2^{(r)}(2) + A_3^{(r)}(H_4)B_3^{(r)}(2) \\ &\quad + A_4^{(r)}(H_4)B_4^{(r)}(2) + A_5^{(r)}(H_4)B_5^{(r)}(2) + A_6^{(r)}(H_4)B_6^{(r)}(2) \\ &= 0 + 0 + 0 + 1 \times DK_4 + 0 + 0 \\ &= DK_4 \end{aligned} \tag{25}$$

4.2 Dynamic access control

When building a digital resource sharing system in a cloud environment, changes in dynamic access control must be addressed. This means that a system might have to add and remove members as well as modify records at any time and in any situation. As an example of a specific change, when a user completes a task, the document is not modified; however, new users may be required to access documents within a limited time. Owners of document records and system administrators can add user rights to access records, delete users with proper authorization, or increase or decrease the access of existing users.

4.3 Add user

When the system adds a user, the CA adds the user's image to the database and updates the user's access rights and the old public polynomials. The steps involved in adding a user are as follows.

Step 1: To add a member S_{n+1}, the CA establishes a secret key H_{n+1}.

Step 2: The CA updates secret polynomial $A_{n+1}^{(r)}(x)$ and indicate function $I_{H_{n+1}}^{(x)}$.

$$A_{n+1}^{(r)}(x)=\left\{\prod_{1\le k\le n,k\ne i}\left[\frac{x-H_k}{H_i-H_k}+\left(x-H_i\right)\right]+d\left(z\,\mathrm{mod}\,24-\mathit{current\,hour}\right)Q\right\}\times I_{H_i}^{(r)},\tag{26}$$
$$i=1,2,\,\ldots,n,x\in R$$

Step 3: If H_{n+1} is a legal secret key, then $A_{n+1}^{(r)}(H_{n+1})=1$; otherwise, it is 0.

$$\theta_{n+1}^{(r)}(x)=I_1^{(A_{n+1}^{(r)}(x))},\ \theta_{n+1}^{(r)}(H_{n+1})=1,\ \theta_{n+1}^{(r)}(\ne H_{n+1})=0\tag{27}$$

Step 4: The CA updates secret polynomial $B_{n+1}^{(r)}(y)$ and indicate function $I_{J_{n+1}}(y)$.

$$B_{n+1}^{(r)}(y)=\left\{\sum_{u\in J_{n+1}}DK_u\left[\prod_{l=1,l\ne u}^{m}\frac{(y-1)}{(u-1)}\right]+d\left(z_{n+1}\,mod\,24-\mathit{current\,hour}\right)Q\right\}\times I_{J_{n+1}}(y),\tag{28}$$
$$y\in R,$$

where J_{n+1} = the number of confidential records that the $(n+1)$th user is authorized to access,

$$I_{J_{n+1}(y)}=\begin{cases}1, & \text{if } y\in J_{n+1},\\ 0, & \text{otherwise.}\end{cases}\tag{29}$$

Step 5: The original public polynomial $G^{(r)}(x,y)$ is updated to

$$\overline{G^{(r)}(x,y)}=G^{(r)}(x,y)+A_{n+1}^{(r)}B_{n+1}^{(r)}(y).\tag{30}$$

4.4 Remove user

To remove user S_k, the CA updates public polynomial G to

$$\overline{\overline{G^{(r)}(x,y)}}=G^{(r)}(x,y)-A_{n+1}^{(r)}B_{n+1}^{(r)}(y)\,. \tag{31}$$

4.5 Add a member at a certain time

When the system adds a user, the CA updates the user's right to access records in a certain time and polynomial $G^{(r)}(x, y)$. The process is as follows.

Step 1: To add member S_{n+1}, the CA creates a secret key H_{n+1}.

Step 2: The CA updates secret polynomial $A_{n+1}^{(r)}(x)$ and indicate function $I_{H_{n+1}}^{(r)}$.

$$\begin{aligned}A_{n+1}^{(r)}(x)=&\left\{\prod_{1\le k\le n,k\ne i}\left[\frac{x-H_k}{H_i-H_k}+\left(x-H_{n+1}\right)\right]+d\left(z_{n+1}\operatorname{mod}24-\mathit{current\,hour}\right)Q_{n+1}\right\}\\&\times I_{H_i}^{(r)},\ i=1,2,\ldots,n,\,x\in R,\end{aligned} \tag{32}$$

where $Q_{n+1}=Q\times\prod_{1\le k\le n,k\ne i,n+1}\left(x-H_{n+1}\right)$.

Step 3: When H_{n+1} is a legal secret key, then $A_{n+1}^{(r)}(H_{n+1})=1$; otherwise, it is 0.

$$\theta_{n+1}^{(r)}(x)=I_1^{(A_{n+1}^{(r)}(x))},\ \theta_{n+1}^{(r)}(H_{n+1})=1,\,\theta_{n+1}^{(r)}(\ne H_{n+1})=0 \tag{33}$$

Step 4: The CA updates secret polynomial $B_{n+1}^{(r)}(y)$ and indicate function $I_{J_{n+1}}(y)$.

$$\begin{aligned}B_{n+1}^{(r)}(y)=&\left\{\sum_{u\in J_{n+1}}DK_u\left[\prod_{l=1,l\ne u}^{m}\frac{\left(y-1\right)}{\left(u-1\right)}\right]+d\left(z_{n+1}\operatorname{mod}24-\mathit{current\,hour}\right)Q_{n+1}\right\}\\&\times I_{J_{n+1}}(y),\ y\in R,\end{aligned} \tag{34}$$

where $Q_{n+1}=Q\times\prod_{1\le k\le n,k\ne i,n+1}\left(x-H_{n+1}\right)$ and

J_{n+1} = {the coding of confidential records that the (n + 1)th user can access}, (35)

where $I_{J_{n+1}(y)}=\begin{cases}1, & \text{if } y\in J_{n+1},\\ 0, & \text{otherwise.}\end{cases}$

Step 5: The original public polynomial $G^{(r)}(x, y)$ is updated to

$$\overline{G^{(r)}(x,y)}=G^{(r)}(x,y)+A_{n+1}^{(r)}B_{n+1}^{(r)}(y)\,. \tag{36}$$

4.6 Add several users at a certain time

When adding several new users to the system, each user has private access. The CA updates the authorization to access a record at a specific time and the public polynomial $G^{(r)}(x, y)$. The process is as follows.

Step 1: To add a member S_{n+1}, the CA creates a secret key H_{n+1}.

Step 2: The CA updates secret polynomial $A_{n+1}^{(r)}(x)$ and indicate function $I_{H_{n+1}}^{(x)}$.

$$A_{n+1}^{(r)}(x)=\left\{\prod_{1\le k\le n,k\ne i}\left[\frac{x-H_k}{H_i-H_k}+\left(x-H_{n+1}\right)\right]+\bar{d}_{m1,m2,\dots,mc}\left(\tilde{z}\bmod 24-current\,hour\right)Q_{n+1}\right\} \\ \times I_{H_i}^{(r)}, i=1,2,\dots,n,\ x\in R, \tag{37}$$

where $Q_{n+1}=Q\times\prod\limits_{1\le k\le n,k\ne i,n+1}\left(x-H_{n+1}\right)$.

For a new user with indices m_1 to m_c, we have

$$\bar{d}_{m1,m2,\dots,mc}=\left(\tilde{z}\bmod 24-current\,hour\right)=\prod_{i=1}^{c}d_i\left(z_i\bmod 24-current\,hour\right). \tag{38}$$

Step 3: When H_{n+1} is a legal secret key, $A_{n+1}^{(r)}(H_{n+1})=1$; otherwise, it is 0.

$$\theta_{n+1}^{(r)}(x)=I_1^{(A_{n+1}^{(r)}(x))},\ \theta_{n+1}^{(r)}(H_{n+1})=1,\ \theta_{n+1}^{(r)}(\ne H_{n+1})=0. \tag{39}$$

Step 4: The CA updates secret polynomial $B_{n+1}^{(r)}(y)$ and indicate function $I_{J_{n+1}}(y)$.

$$B_{n+1}^{(r)}(y)=\left\{\sum_{u\in J_{n+1}}DK_u\left[\prod_{l=1,l\ne u}^{m}\frac{\left(y-1\right)}{\left(u-1\right)}\right]+\bar{d}_{m1,m2,\dots,mc}\left(\tilde{z}\bmod 24-current\,hour\right)Q\right\} \\ \times I_{J_{n+1}}(y),\ y\in R \tag{40}$$

where $Q_{n+1}=Q\times\prod\limits_{1\le k\le n,k\ne i,n+1}\left(x-H_{n+1}\right)$.

For a new user with indices m_1 to m_c, we have

$$\bar{d}_{m1,m2,\dots,mc}=\left(\tilde{z}\,mod\,24-current\,hour\right)=\prod_{i=1}^{c}d_i\left(z_i\bmod 24-current\,hour\right) \tag{41}$$

and

$$J_{n+1}=\{\text{the coding of confidential records that the } (n+1)\text{th user can access}\}, \tag{42}$$

where $I_{J_{n+1}(y)}=\begin{cases}1, & \text{if } y\in J_{n+1},\\ 0, & \text{otherwise.}\end{cases}$

Step 5: The original public polynomial $G^{(r)}(x, y)$ is updated to

$$\overline{G^{(r)}(x,y)} = G^{(r)}(x,y) + A_{n+1}^{(r)} B_{n+1}^{(r)}(y)\,. \tag{43}$$

5. Security Analysis

The access rights of multiple users and author copyright problems must be addressed in cloud-based digital teaching systems. Because a cloud storage system allows random revision and resource sharing, security and stability become essential. The core features of managing data access in a cloud storage system are public key encryption, the Lagrange interpolation polynomial, and the access control matrix, as discussed above, and unauthorized keys are protected by symmetric encryption. The Lagrange interpolation polynomial is used to compare and verify public key cryptosystems. Users must pass an image recognition test to access the access control matrix to obtain authorization for access from the CA in this system. Each user has their right of access, and if they want to access the matrix access data of other users, they must simultaneously crack access polynomials or a Lagrange interpolation polynomial as well as the public key cryptography system.

Previous research has focused on the development of polynomials to control access rights. However, repeated calculation and reconstruction of access polynomials upon various updates and changes in the composition of users will increase the calculation complexity of a system. The polynomial in this study is repeatedly applied in the reconstruction algorithms required after each update. The access control matrix proposed in this study helps decrease the computational load of the dynamic update system, and adding new parameters and a timestamp to the access control matrix can effectively increase the security of a system.

User access rights, security problems, and common attacks, including internal, external, integration, and equation attacks, are discussed and analyzed in this section.

5.1 External attack

An external attack is an attack on a system through the public decryption polynomial. The attacker acquires decryption information by using the decryption polynomial to crack a verified indicate function to acquire a user's key to steal confidential records.

For an external attack, the public decryption polynomial $G^{(r)}(x, y)$ and user codes are the only two means by which attackers can acquire decryption information. In contrast to $G^{(r)}(x, y)$, $A_i^{(r)}(x)$ and $B_i^{(r)}(y)$ are secret polynomials. When someone attempts to crack the indicate function, $A_i^{(r)}(x)$ and $B_i^{(r)}(y)$ must be solved. Moreover, the user code lacks the decryption information required to access a document and the user's private key cannot be acquired by a reverse calculation. The same situation occurs when adding users. As described in the security test of decryption polynomial $G^{(r)}(x, y)$, attackers cannot calculate the arithmetic formula of the decryption key through derivation. Moreover, a timestamp enhances the complexity of equations. The difficulty of cracking the system is enhanced if it must be achieved within a limited time. External attackers cannot successfully acquire user data and confidential document records externally.

5.2 Internal attack

An internal attack is one in which a legal user (S_i) of an internal system with a low level of authorization attempts to acquire the key with a higher level of authorization. The user therefore attempts to acquire increased access through a public decryption polynomial $G^{(r)}(x, y)$ and the private key (H_i) to access confidential records beyond their authorization.

In the access control matrix of members in Fig. 4, user S_2 can access records $file_2$, $file_3$, $file_4$, and $file_5$ and user S_3 can access records $file_1$ and $file_3$, i.e., user S_3 has less access than user S_2. There is a partial order relation between S_2 and S_3, denoted $S_3 \leq S_2$, showing that S_2 has higher access right ($S_2 = \{2,3,4,5\}$; $S_3 = \{1,3\}$), and user S_3 is a potential attacker of S_2. S_3 tries to input secret key H_3 into public decryption polynomial $G^{(r)}(x, y)$ to acquire key H_2 of user S_2 to access confidential documents $file_2$ and $file_4$, which require a higher authorization level.

In the calculation of the user's private key, user S_3 could substitute (H_3, 1) and (H_3, 3) into public polynomial $G^{(r)}(x, y)$ to acquire decryption keys DK_1 and DK_3 and access confidential records $file_1$ and $file_3$. Nevertheless, the user must have the authorization of user S_2 to acquire decryption keys DK_3, DK_4, and DK_5 to access $file_2$, $file_4$, and $file_5$, respectively.

Since user S_3 has the lower authorization level, S_3 must attack the secret polynomial in the system to acquire decryption keys DK_2, DK_4, and DK_5 of S_2 to attack H_2 in $A_2^{(r)}(x)$ and decryption keys DK_2, DK_3, and DK_5 in $B_2^{(r)}(y)$. User S_3 can substitute the private key H_3 into decryption polynomial $G^{(r)}(x, y)$ and acquire decryption keys DK_1 and DK_3, as expressed by the following calculation.

$$\begin{gathered} G^{(r)}(H_3,1) = DK_1 \\ \Rightarrow G^{(r)}(H_3,1) - DK_1 = 0 \\ \Rightarrow A_1^{(r)}(H_3)B_1^{(r)}(1) + A_2^{(r)}(H_3)B_2^{(r)}(1) + \cdots + A_5^{(r)}(H_3)B_5^{(r)}(1) - DK_1 = 0 \end{gathered} \tag{44}$$

$$\begin{gathered} G^{(r)}(H_3,3) = DK_3 \\ \Rightarrow G^{(r)}(H_3,3) - DK_3 = 0 \\ \Rightarrow A_1^{(r)}(H_3)B_1^{(r)}(3) + A_2^{(r)}(H_3)B_2^{(r)}(3) + \cdots + A_5^{(r)}(H_3)B_5^{(r)}(3) - DK_3 = 0 \end{gathered} \tag{45}$$

$$\begin{array}{c|ccccc|} & file_1 & file_2 & file_3 & file_4 & file_5 \\ S_1(H_1) & 1 & 1 & 1 & 1 & 1 \\ S_2(H_2) & 0 & 1 & 1 & 1 & 1 \\ S_3(H_3) & 1 & 0 & 1 & 0 & 0 \\ S_4(H_4) & 0 & 0 & 1 & 1 & 0 \\ S_5(H_5) & 0 & 0 & 0 & 0 & 1 \end{array}$$

Fig. 4. Member access matrix.

In addition to needing to acquire many numbers and the arithmetic formulas $A_3^{(r)}(H_3)B_3^{(r)}(1)$ and $A_3^{(r)}(H_3)B_3^{(r)}(3)$, which cannot easily be obtained, the attacker cannot obtain by reverse reasoning the secret key H_2 of S_2 or acquire decryption keys DK_2, DK_4, and DK_5. Since the personal verification index of user S_2 protects the secret polynomial $A_2^{(r)}(x)B_2^{(r)}(y)$, even if the attacker acquires this secret polynomial, they cannot crack $A_2^{(r)}(x)$ and $B_2^{(r)}(y)$, which are protected by the verification index.

Assume that attacker S_3 attempts to acquire H_2-related information $A_2^{(r)}(x)$ hidden in the polynomial.

$$\begin{aligned} A_2^{(r)}(x)=\Bigg\{&\left[\frac{x-H_1}{H_2-H_1}+(x-H_2)\right]\times\left[\frac{x-H_3}{H_2-H_3}+(x-H_2)\right]\times\left[\frac{x-H_4}{H_2-H_4}+(x-H_2)\right]\\ &\times\left[\frac{x-H_5}{H_2-H_5}+(x-H_2)\right]+d\left(z \bmod 24-current\ hour\right)Q\Bigg\}\times I^{(x)}_{\{H_1,\ldots,H_5\}} \end{aligned} \tag{46}$$

Then, the CA authorizes a user with personal secret polynomial $A_i^{(r)}(x)$ with a verified indicate function to confirm the existence of the user in the list and the possession of the access right and the legal secret key H_i. Users that are not authorized by the CA cannot pass the examination of index $I^{(x)}_{\{H_1,\ldots,H_n\}}$ of $A_i^{(r)}(x)$. Furthermore, when a user is a legally authorized user in the CA list but uses a non-personal key H_i in the decryption polynomial, the CA blocks the user from acquiring authorization. In the following example, user S_3 with secret key H_3 can access records *file*$_1$ and *file*$_3$; when the user intends to use a private key in $A_2^{(r)}(x)$, the user is blocked during the verification of $\theta_i^{(r)}(x)=I_1^{(A_i^{(r)}(x))}$ and acquires meaningless maximal values, while the indicate function shows a value of 0, preventing the attacker from finding a clue to crack the system.

User S_3 has to attack DK_2, DK_4, and DK_5 in secret polynomial $B_2^{(r)}(y)$ to acquire records *file*$_2$, *file*$_4$, and *file*$_5$, respectively. In this case, user S_3 can only attack with their personal key S_3 = {1,3} but cannot pass the verification J_2 = {2,4,5} of $I_{J_2}(y)$; a value of 0 is output and the attack fails to acquire the access key.

According to the above verification, an attacker cannot acquire decryption information from the reverse partial polynomial. The method proposed in this study can effectively prevent internal attackers from breaching the information security of the system.

5.3 Integration attack

Integration attackers are two or more system users authorized by the CA who cooperatively attack the system similarly to an internal attack, whereas internal attacks are instigated by only one authorized attacker. Compared with an internal attack, an integration attack involves more attacks. In the CA system, there is partial order relation among users. An integration attack aims to use the attackers' secret keys and those of other internal users to calculate arithmetic formulas to acquire unauthorized document records. Two scenarios are considered: one is that two or more collaborative attackers obtain an internal member's key with a partial order relation, and the other is that members without an order relation gain an internal member's key.

Users S_3 and S_4 have a lower authorization level than user S_1 and attempt to access records *file*$_2$ and *file*$_5$. Figure 5 demonstrates that attackers S_3 and S_4 with access {1,4} and {3,4}, respectively, intend to attack user S_1 with access {1,2,3,4,5}, i.e., a user with a higher level of authorization according to the partial order relation. Attackers aim to acquire user S_1's records *file*$_2$ and *file*$_5$ and decryption keys DK_2 and DK_5 through their decryption information, where the decryption information related to keys DK_2 and DK_5 is hidden in $A_2^{(r)}(x)B_2^{(r)}(y)$.

$$A_2^{(r)}(x)=\left\{\left[\frac{x-H_1}{H_2-H_1}+\left(x-H_1\right)\right]\times\left[\frac{x-H_3}{H_2-H_3}+\left(x-H_3\right)\right]\times\left[\frac{x-H_4}{H_2-H_4}+\left(x-H_4\right)\right]\right.$$
$$\left.\times\left[\frac{x-H_5}{H_2-H_5}+\left(x-H_5\right)\right]+d\left(z\bmod 24-\mathit{current\,hour}\right)Q\right\}\times I_{H_2}^{(r)} \tag{47}$$

$$B_2(y)=\begin{bmatrix} DK_2\times\dfrac{(y-1)(y-3)(y-4)(y-5)}{(2-1)(2-3)(2-4)(2-5)} \\ +DK_3\times\dfrac{(y-1)(y-2)(y-4)(y-5)}{(3-1)(3-2)(3-4)(3-5)} \\ +DK_4\times\dfrac{(y-1)(y-2)(y-3)(y-5)}{(4-1)(4-2)(4-3)(4-5)} \\ +DK_5\times\dfrac{(y-1)(y-2)(y-3)(y-4)}{(5-1)(5-2)(5-4)(5-4)} \end{bmatrix}$$
$$\times I_{J_2}(y)+d\left(x\bmod p+TS(t)-\mathit{current\,time}\right)Q\times I_{J_2}^{(y)} \tag{48}$$

Attackers S_3 and S_4 can obtain secret keys H_3 and H_4 given by the system. H_2 cannot be acquired through $A_2^{(r)}(x)$. In attempt to crack the system, a string of meaningless numbers will appear after substituting the key. Moreover, in the verification of $\theta_i^{(r)}(x)=I_1^{(A_i^{(r)}(x))}$, the final result will be 0 and the attacker will not obtain any clues to crack the system.

$$\begin{array}{c|ccccc} & \mathit{file}_1 & \mathit{file}_2 & \mathit{file}_3 & \mathit{file}_4 & \mathit{file}_5 \\ S_1(H_1) & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} \\ S_2(H_2) & \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} \\ S_3(H_3) & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} \\ S_4(H_4) & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{0} \\ S_5(H_5) & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} \end{array}$$

Fig. 5. Coordinated attackers and the attacked partial order relation.

As described above, an integration attack, a single attack. and a partial order relation among two or more cooperative attackers cannot be used to acquire decryption information and clues, regardless of the number of cooperative attackers.

For example, users S_3 and S_4, with a lower level of authorization, can access specific records but not records requiring a higher level of authorization. They attempt to acquire *file*$_5$, which can only be acquired with a higher level of authorization such as that given to special units or institutes.

Figure 5 reveals that the coordinated attackers and the attacked do not show a partial order relation. A partial relation is set in the CA system so that $S_5 = \{5\}$ becomes the target of attackers $S_3 = \{1,4\}$ and $S_4 = \{3,4\}$. The access level does not make a difference in this situation. The attackers therefore try to use the decryption information to increase the probability of cracking private key DK_5 and acquiring the confidential document *file*$_5$. The decryption key DK_5 is hidden in $A_5^{(r)}(x)B_5^{(r)}(y)$.

$$\begin{aligned} A_5^{(r)}(x) = {} & \left[\frac{x-H_1}{H_5-H_1}+\left(x-H_1\right)\right]\times\left[\frac{x-H_2}{H_5-H_2}+\left(x-H_2\right)\right]\times\left[\frac{x-H_3}{H_5-H_3}+\left(x-H_3\right)\right] \\ & \times\left[\frac{x-H_4}{H_5-H_4}+\left(x-H_4\right)\right]+d\left(z \bmod 24-\mathit{current\,hour}\right)Q\Bigr\}\times I_{H_5}^{(r)} \end{aligned} \tag{49}$$

$$\begin{aligned} B_5(y) = {} & \left[DK_5\times\frac{(y-1)(y-2)(y-3)(y-4)}{(5-1)(5-2)(5-3)(5-4)}\right]\times I_{J_5}(y) \\ & +d\left(x \bmod p+TS(t)-\mathit{current\,time}\right)Q\times I_{J_5}^{(y)} \end{aligned} \tag{50}$$

Attackers performing the derivation cannot acquire information through partial secret keys H_3 and H_4. Substituting these two keys into $A_5^{(r)}(x)$ does not enable them to acquire H_5, and they obtain a string of unsolvable numbers. Moreover, because $\theta_i^{(r)}(x) = I_1^{(A_i^{(r)}(x))}$, a value of 1 would not be obtained, enabling them to acquire information from $A_5^{(r)}(x)B_5^{(r)}(y)$. According to the result of applying the algorithm, regardless of the order among the members or the number of attacks, attackers cannot acquire the targeted key or decryption key of document records. An integration attack therefore cannot crack the system.

5.4 Equation attack

An equation attack refers to attackers attempting to use the public decryption polynomial $G^{(r)}(x, y)$ to acquire the private key with improper mathematical methods. This type of attack might easily occur while changing a user's access level, such as when the system adds, removes, or modifies members with access to particular confidential documents. In this attack, the attacker seeks opportunities to crack or intercept public polynomials by changing them. As a result, the security of access modification is at the core of this attack. Here, the types of modification discussed earlier are thoroughly examined.

1. Add members:

$$\overline{G^{(r)}(x,y)} = G^{(r)}(x,y) + A_{n+1}^{(r)}(x)B_{n+1}^{(r)}(y) \tag{51}$$

When a system adds a user, attackers can deduce the updated public decryption polynomial $G^{(r)}(x, y)$ from the original decryption polynomial $G^{(r)}(x, y)$. $A_{n+1}^{(r)}(x)B_{n+1}^{(r)}(y)$ and the polynomial result were discussed in Sect. 3.2. If attackers attempt to crack this expression, a string of meaningless numbers will appear. For this reason, attackers cannot crack the decryption information or acquire any records of users.

2. Remove members:

$$\overline{\overline{G^{(r)}(x,y)}} = G^{(r)}(x,y) - A_k^{(r)}(x)B_k^{(r)}(y) \tag{52}$$

Similar to adding members, attackers can deduce the updated public polynomial $\overline{G^{(r)}(x,y)}$ from the original polynomial $G^{(r)}(x,y)$ when the system removes a member. However, the attackers still cannot derive $A_{n+1}^{(r)}(x)B_{n+1}^{(r)}(y)$.

3. Modify access rights:

$$\widetilde{G^{(r)}(x,y)} = G^{(r)}(x,y) - A_i^{(r)}(x)B_i^{(r)}(y) + A_i^{(r)}(x)B_i^{\prime(r)}(y) \tag{53}$$

In the process of modifying access authorization, attackers can acquire $A_i^{(r)}(x)B_i^{(r)}(y) - A_i^{(r)}(x)B_i^{\prime(r)}(y)$ by deducing old and new public polynomials. Although the result is different from that in the previous two attacks, the reason for not being able to crack the system is the same. Even though $x = 0$ or $y = 0$ is set, the acquired result will be a huge string of meaningless values. Even an attacker attacking during the modification of a user's access modification cannot crack the relevant decryption information. Thus, it appears that attackers cannot acquire relevant decryption information during the modification of access authorization.

According to the above security analyses, four common types of attackers are unable to successfully crack the secure access control mechanism proposed in this study, and no decryption information is leaked as a result of these attacks. Thus, the system can successfully protect itself from attack, ensuring its security.

6. Conclusions

We propose a technique based on timestamps and coupled with a security access control mechanism for use with cloud e-learning platforms. It aims to provide stable and secure cloud-based digital resource access platforms for universities to promote teaching quality, enhance the interaction between teachers and students, and achieve ubiquitous learning through platforms. First, image recognition is employed to identify possibly illegal users, then the characteristics of the Lagrange interpolation polynomial are employed to divide the access rights of users into different levels to propose methods for solving cloud computing problems, such as responding to access requests from users with different levels of authorization at the same time.

The application of timestamps is also integrated into this study to create a complete access control structure and effectively improve access to cloud digital resources. The novelty of this study is that it incorporates timestamps and an access control mechanism into cloud-based e-learning platforms. This has the advantage of solving the problem of access requests from different users during cloud computing. Moreover, the system also minimizes the complexity of security management while preventing successful attacks. Furthermore, users cannot access or randomly modify the authorization settings, ensuring a complete and secure cloud-based digital resource access system.

Because of its secure encryption, the proposed cloud-based digital resource sharing system combines instantaneity, effectiveness, and stability of time and location. Furthermore, the digital material resources provided by cloud-based e-learning platforms are protected by copyright while allowing a wide range of users to access resources regardless of the time, space, and location. Teachers can use students' learning plans to improve their learning environment and assist them in learning more effectively.

In the digital material access and delivery process, access control management and system compatibility are major concerns. The sharing of complete cloud digital resources can benefit from secure and stable data management and sharing solutions. This study demonstrates the security of system access control and the reliability of the system services by analyzing four common types of attack: external, internal, integration, and equation attacks. The results of this study provide a more effective technique for optimizing e-learning while simultaneously improving the quality of digital sharing.

Compared with previous systems,(15) in this research, we add dynamic access control and the ability to add and delete users as well as image recognition. Combined with IoT technology, the platform can filter out most attacks. The image recognition has an accuracy rate of about 85%, is capable of identifying valid users, and includes a Lagrange security mechanism to protect the system from both internal and external attacks.

References

1 Taking IT to the Next Normal with Future IT: https://blogs.idc.com/2021/05/03/taking-it-to-the-next-normal-with-future-it/ (accessed October 2021).

2 A. Tymochko, S. Dudenko, O. Bodiak, and A. Perepelitsa: 2018 IEEE 9th Int. Conf. Dependable Systems, Services and Technologies (IEEE, 2018) 539–543. https://doi.org/10.1109/DESSERT.2018.8409191

3 T. Y. Lin and P. Vachon: 2017 IEEE Int. Conf. Big Data (IEEE, 2017) 1821–1829. https://doi.org/10.1109/BigData.2017.8258126

4 D. F. Ferraiolo, R. S. Sandhu, S. I. Gavrila, D. R. Kuhn, and R. Chandramouli: ACM Trans. Inf. Syst. Secur. **4** (2001) 224. https://doi.org/10.1145/501978.501980

5 G. Coulouris, J. Dollimore, and M. L. Roberts: Proceedings of the third ACM Workshop on Role-based Access Control (ACM, 1998) 115–121. https://doi.org/10.1145/286884.286908

6 S. Shohieb and H. K. Elminir: Intell. Autom. Soft Comput. **21** (2015) 211. https://doi.org/10.1080/10798587.2014.966456

7 K. Lu and X. Zhang: 2010 Int. Conf. Artificial Intelligence and Computational Intelligence (AICI, 2010) 219–223. https://doi.org/10.1109/AICI.2010.53

8 M. Pantic and L. J. M. Rothkrantz: IEEE Trans. Systems, Man, and Cybernetics, Part B (Cybernetics) 1449–1461. https://doi.org/10.1109/*TS*MCB.2004.825931

9 R. Sandhu and Q. Munawer: Proceedings 14th Annual Comput. Security Applications Conf. (ACSAC, 1998) 39–49. https://doi.org/10.1109/CSAC.1998.738569

10 R. S. Sandhu and P. Samarati: IEEE Commun. Mag. **32** (1994) 40. https://doi.org/10.1109/35.312842

11 S. H. Tang, X. Y. Li, X. Y. Huang, X. Yang, and X. Lingling: IEEE Trans. Computers (IEEE, 2015) 2325. https://doi.org/10.1109/TC.2015.2479609

12 J. S. Park, K. P. Costello, T. M. Neven, and J. A. Diosomito: Proc. 9th ACM Symp. Access Control Models and Technologies (SACMAT, 2004) 163–172. https://doi.org/10.1145/990036.990063

13 Y. F. Chung, H. H. Lee, F. P. Lai, and T. S. Chen: Info. Sci. **178** (2008) 230. https://doi.org/10.1016/j.ins.2007.08.001

14 D. Hans and K. Helmut: Introduction to Cryptography (Springer, Deutschland, 2007) 2nd ed., Chap. 3. https://doi.org/10.1007/3-540-49244-5

15 T. C. Hsiao, Z. Y. Wu, T. L. Chen, Y. F. Chung, and T. S. Chen: Int. J. Distrib. Sens. Netw. **14** (2018) 1. https://doi.org/10.1177/1550147718790892

About the Authors

Yao-Min Huang received his Master's degree in information management from Tunghai University in 2014. He is currently a Ph.D. student of the Department of Management Science, National Yang Ming Chiao Tung University, focusing on information management, financial management, deep learning, and information security.

Yu-Fang Chung received her B.A. degree in English language, literature, and linguistics from Providence University in 1994, her M.S. degree in computer science from Dayeh University in 2003, and her Ph.D. degree in computer science from National Taiwan University, Taiwan, in 2007. She is currently a professor of the Department of Electronic Engineering and Information Management, Tunghai University, where she is involved in research on information security and cryptography.

Dai-Lun Chiang received her Ph.D. degree in biomedical electronics and bioinformatics from National Taiwan University in 2020. She is currently an assistant professor at the Financial Technology Applications Program, Ming Chuan University. Her main research areas include financial technology, information security, bioinformatics, and machine learning.

Ya-Hsin Chang received her B.A. degree from the Foreign Language and Literature Department, Tunghai University in 2019 and her Master's degree in information management from Tunghai University in 2020. Her research currently involves information security and management.

Tzer-Shyong Chen received his Ph.D. degree in computer science from the Department of Electrical Engineering, National Taiwan University, Taiwan, in 1996. He is currently chair of the Department of Information Management, Tunghai University, Taiwan. He has served on an evaluation committee of the Institute of Electrical Engineering Taiwan and is also a member of IEEE. He has authored/co-authored over 80 refereed publications. His main research interests are information security, cryptography, and network security.

Chih-Cheng Chen is a professor at Jimei University, China. He is a senior member of IEEE. He earned his Ph.D. degree in mechatronics engineering from National Changhua University of Education. He has published 43 articles and owns three patents. He is currently researching RFID application systems, AIoT, machine learning, and information security.