A Remote Access Control Method for Electronic Financial Management Data Based on Object Attribute Matching

Xue Yuan(✉) and Zimin Bao

Department of Management, Xi'an Jiaotong University City College, Xi'an 710018, China
xycy272@163.com

Abstract. In response to the shortcomings of existing data remote access control methods such as long private key generation time and high packet loss rate in remote control, this paper proposes an electronic financial management data remote access control method based on object attribute matching. Firstly, analyze the connotation of role-based access control and determine the object attributes for accessing electronic financial management data; Secondly, set the access permission category for electronic financial management data files and match the object attributes of external access control; Once again, the weight assignment method of double coefficient of variation is used to assign weights to electronic financial management data, and a secure access control model is designed based on attribute encryption; Finally, a recursive algorithm is used to decrypt and control remote access, completing the design of a remote access control method for electronic financial management data based on object attribute matching. Through experiments, it has been proven that the average private key generation time of the proposed method for accessing electronic financial management data is about 205ms, and the packet loss rate of remote control is always below 1.0%, indicating good application performance.

Keywords: Object Attributes · Access Control · Attribute Matching · Weight Assignment · Decryption Control

1 Introduction

With the rapid development of information technology and the popularization of electronic financial management, more and more enterprises and organizations tend to store financial data in electronic systems. These data include sensitive data such as financial statements, transaction records, and customer information. However, remote access to these financial data also brings a series of security risks and challenges, making the research and implementation of remote access control methods for electronic financial management data crucial [1].

Firstly, the security of financial data is crucial for the operation and reputation of enterprises and organizations. Unauthorized access may lead to data leakage, tampering,

L. Yun et al. (Eds.): ADHIP 2023, LNICST 547, pp. 409–421, 2024.
https://doi.org/10.1007/978-3-031-50543-0_28

or loss, causing significant losses to the enterprise. Therefore, effective access control methods are needed to ensure that only authorized users can remotely access financial data, and encryption and other security measures are taken to protect the confidentiality and integrity of the data. Secondly, the demand for remote access is an important factor driving the development of remote access control methods for electronic financial management data [2]. Finally, the development of access control technology provides technical support for remote access control methods for electronic financial management data. Technologies such as authentication, permission management, and encrypted communication can be used to ensure that only authorized users can remotely access financial data and protect the security of data during transmission and storage.

Access control not only ensures the security of information and data, but also serves as an important means of authentication and authorization for visitors. Therefore, relevant scholars have designed a series of access control technologies. Currently, role-based access control (RBAC) [3] and attribute based access control (ABAC) [4] are widely used. In RBAC, the system sets different roles in advance and assigns corresponding permissions to them. Users and roles adopt a many to many relationship. Due to the relatively closed early system, there were not many types of roles, which effectively reduced management costs. At the same time, the existence of roles also facilitates the development of security policies by enterprises. In relatively small network environments, RBAC performs well, but with the expansion of network scale and the rise of cloud computing IoT, RBAC is becoming increasingly difficult to meet demand. A large number of network nodes make network management extremely complex. RBAC is difficult to achieve fine-grained access. Administrators cannot predict in advance how many kinds of users will apply for access, nor can they fully consider the role permission correspondence. The attribute based access control (ABAC) scheme provides a new idea. It binds the control policy and the user attribute together. Only the attribute set satisfies the control policy can the resource be accessed. Some researchers have proposed an access control model of role matching in distributed workflow environment. Based on different tasks of workflow, this model can search for one or more groups of role sets with relevant task execution permissions from system roles, and then carry out matching optimization by referring to the environment, time constraints and inheritance relationship between roles, and finally select the optimal role set for users [5]. However, this method may be affected by the surrounding environment, which prolongs the private key generation time and affects the effect of remote access control. Some researchers have proposed a smart grid electricity data access control method based on the ABAC access control model. A dynamic context authorization strategy based on the ABAC access control model was implemented in the WSO2 system using XACML policy language, which can meet the context based dynamic access characteristics of smart grid environments [6]. However, in the practical application of remote control, this access control method may lead to an increase in the system's packet loss rate and reduce the effectiveness of remote access control.

Therefore, in order to further improve the security of access control mechanism, this paper combines the access control method based on attributes and roles, and proposes a remote access control method for electronic financial management data based on object attribute matching.

2 Role-Based Access Control and Attribute-Based Access Control

2.1 Role-Based Access Control

RBAC, or Role Based Access Control, is an access control mechanism widely used in computer security. It controls users' access to resources by assigning roles to users. In RBAC, a role is a set of permissions that can be divided based on a user's job responsibilities or positions, and each role can be authorized to one or more users. Users can only access the permissions of their roles when using resources, without specifying whether they have specific access permissions. This approach greatly simplifies administrator tasks and improves system security by encapsulating the permissions of each user [7].

RBAC can help organizations effectively manage access to resources, dictate who can do what and when, ensure that the system is only used by authorized personnel, and facilitate administrators' management of users and their roles. RBAC also reduces human error and administrative costs, improving system reliability and security. This mechanism has been widely used not only in computer operating system and network system, but also in many other fields, such as enterprise, medical, education, finance and so on. In RBAC, roles are mainly divided into subject and object, which refer to users (or processes), and object refers to permissions and resources (or objects). Subject obtains authorization through roles, so that it can operate objects [8]. In RBAC, a principal can have multiple roles, and a role can contain multiple permissions; An object can also be accessed by multiple roles, and a permission can be granted to multiple roles. This mechanism makes the management of roles, permissions, and resources more flexible and efficient, while also improving the security of the system. In a database system, administrators can define multiple roles, such as super administrators, system administrators, regular users, etc. Authorize these roles to different user groups or individuals, and different users can use their respective roles for authorization operations.

2.2 Attribute-Based Access Control

ABAC (Attribute-Based Access Control) is an access control mechanism widely used in computer systems. Unlike RBAC, ABAC controls users' access to resources through attributes rather than assigning roles to users. In ABAC, users, resources, and environments can all be assigned attributes that can be used in access control decisions. The access request contains user attributes and resource attributes. The system determines whether the user is authorized to access resources based on these attributes. This method can not only achieve more accurate and dynamic access control, but also adapt to different scenarios and application requirements [9].

ABAC is a flexible access control mechanism that can adapt to complex and ever-changing application scenarios, and can more finely control user access to resources, thereby improving system security. As a result, ABAC has been widely applied in many large organizations and enterprises, cloud computing environments, the Internet of Things, and industrial automation fields.

2.3 Access Control Based on Role Attributes

RABAC is a role and attribute based access control model, which refers to the extension of role based access control and attributes. It is an extended access control model that combines RBAC and ABAC. In RBAC, access control decisions are only based on the user's role, without considering the user's attributes; ABAC focuses on user attributes and corresponding user permissions. In RABAC, access control decisions are not only based on user roles, but also on user attributes. In the RABAC model, roles are no longer the only authorization criteria, and users also need to meet certain attribute conditions to obtain access to a resource [10].

At the heart of the RABAC model is the integration of user attributes and role assignment. Users can have multiple attributes, and each attribute can be associated with one or more roles. Each role contains not only a set of operation permissions, but also a set of attribute restrictions. When a user initiates a resource access request, the system makes access control decisions based on the attributes and roles of the user. RABAC is more flexible in defining access control policies by taking into account user attributes than the RBAC model. By introducing attribute conditions, the RABAC model can simplify the complexity of user access control management by using the abstraction mechanism of roles, and at the same time, give full play to the important role of user attributes in access control, improve the degree of refinement of access control, and better meet the actual demand for access control.

Therefore, this paper combines the characteristics of RBAC and ABAC and applies the RABAC model in remote access control of electronic financial management data based on object attribute matching, so as to better meet the current complex network environment and diversified authorization needs.

3 Design of Remote Access Control Method for Electronic Financial Management Data

3.1 Object Attribute

The object owner has supervisory authority and is able to proactively select data visitors, which to some extent ensures users' control over the privacy of electronic financial management data.

The data contributor sets the access permission level for the electronic financial management data file, and calculates its weighted value based on this access permission level, which allows visitors to obtain the lowest weighted value of the electronic financial management data file and store it in the file. When there is an access request, the weighted calculation results of the application access permissions of the data visitor are compared with the weighted permission values calculated from many electronic financial management data files in the database that have already been set with access permissions, and the electronic financial management data files that meet the access permissions of the data visitor are selected. The object matching information flow diagram is shown in Fig. 1.

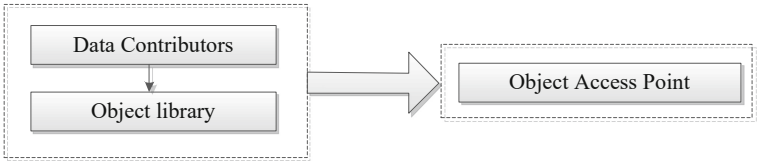

Fig. 1. Object matching information flow diagram

The specific steps are as follows:

(1) The data contributor sets the minimum access permission value of the data to be uploaded, calculates the weighted permission value, writes it into the file, and then uploats the data to the Object Library (OL);
(2) Receive the weighted permission value of the data visitor from the second part and also pass it into the object database OL;
(3) According to the permission threshold set by the contributor, the Object database queries and screens the database, and sends the relevant object data meeting the permission of the visitor to the Object Access Point (OAP) in the second part.

3.2 External Access Control Object Attribute Matching

If you want to access electronic financial management data, when designing External Access Control (EAC), you need to use attribute centered RABAC access control, which takes the role of the object as an attribute to express a user's permission. Due to the fact that various external institutions and types of data visitors belong to cross domain data access, a unified external interface is provided for external visitors. In the institutional system in which it is located, if there is already an access control mechanism (whether it is Discretionary Access Control (DAC), Mandatory Aces Control (MAC), RBAC, ABAC, or other access control mechanisms), the permissions it possesses are represented through the EAC section at the unified external interface, and then transferred to the Level Management Table (LMT), Perform permission ID comparison and matching on the attribute values of the object to access electronic financial management data.

The electronic financial management data file access permission is set as "top secret", "confidential", "secret", "sensitive" and "open" five categories. The access control permission of Top Secret is the highest. The access control permission of Secret, Secret, and Sensitive is decreasing. The access control permission of Public is not required. Write the preceding five categories to the LMT. The level authorization table Settings are shown in Table 1.

The access permission of electronic financial management data files is inclusive. If a user has access permission of "top secret" files, that is, permission ID = 1, he has the right to access four categories of files: "confidential", "secret", "sensitive" and "open". Similarly, the user has "confidential" file access permission, that is, if the permission ID = 2, the user has the right to access the three categories of "secret", "sensitive" and "public" files.

Table 1. Level authorization table

User class	Privilege level	Permission ID
Government department	Top secret	1
Research institutes	Confidential	2
Medical institution	Secret	3
Business organization	Sensitive	4
Individual users	Open	5

If a user wants to access electronic financial management data across permissions, they need to use access control mechanisms within their own domain to obtain their personal corresponding permissions. According to their object attributes, the highest level of access permissions that can be obtained by their organization cannot exceed. The specific access control information flow diagram is shown in Fig. 2.

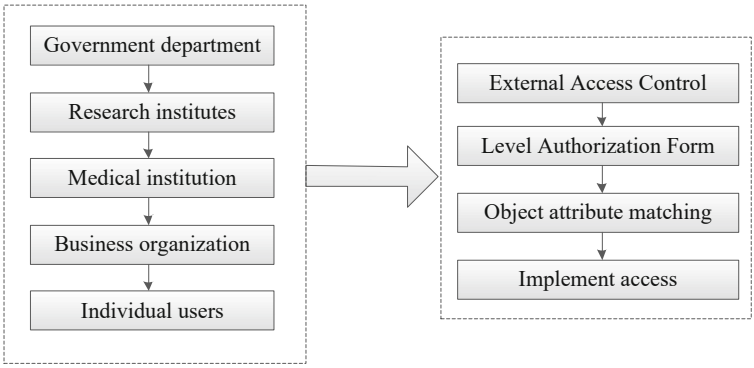

Fig. 2. Access control information flow diagram

The specific steps are as follows:

① The user obtains permissions through the access control system in the domain and accesses the accessible system through the external access control module.

② The EAC formats user permissions, generates unified files, and sends them to the level authorization table.

③ The LMT compares the attribute permissions in the file, matches the object attribute permissions, informs the visitor of the permission result, and generates an ID corresponding to the permission for the visitor, and writes the ID to the permission file.

3.3 Double Coefficient of Variation Weight Assignment Method

In RABAC, as the amount of electronic financial management data increases, changes in access permissions for various types of data will increase the complexity of matching

access permissions. To solve this problem, this article uses the double coefficient of variation weight assignment method to assign weights to electronic financial management data, simplifying the difficulty of matching object attributes and improving matching speed.

At the present stage, there are differences in the representation and dimensionality of each object attribute value, but in the access control attribute matching, these attribute values need to be evaluated and compared horizontally and vertically. In order to improve the practical application effect, it is necessary to normalize the data with dimensionless quantization. Permission values that are already in the range of [0,1] are no longer processed. Instead, the permission value not within the range of [0,1] is normalized using formula (1). The calculation formula is as follows:

$$e_{ij} = \begin{cases} \dfrac{a_{ij} - (a_{ij})_{\min}}{(a_{ij})_{\max} - (a_{ij})_{\min}}, a_{ij}\text{Forward incremental} \\ \dfrac{(a_{ij})_{\max} - a_{ij}}{(a_{ij})_{\max} - (a_{ij})_{\min}}, a_{ij}\text{Forward decreasing} \end{cases} \tag{1}$$

Among them, a_{ij} is the original value; e_{ij} is the quantified value; $(a_{ij})_{\max}$ is the maximum original value; $(a_{ij})_{\min}$ is the minimum value of the original value.

The weight of the coefficient of variation weight assignment method is directly obtained by calculating the information of each indicator. To eliminate the differences between different dimensions of attribute values before calculation, the electronic financial management data is first quantified and processed. Assuming that the quantified electronic financial management data matrix is $Y = (y_{ij})_{m\times n}$, m represents the number of evaluation plans; n represents the number of indicators, so the calculation of the average value $\overline{y}_j$ of each column vector and the standard deviation S_j of each column vector is shown in Formulas (2) and (3):

$$\overline{y}_j = \frac{1}{m}\sum_{i=1}^{m} y_{ij} \tag{2}$$

$$S_j = \sqrt{\frac{1}{m}\sum_{i=1}^{m}\left(y_{ij} - \overline{y}_j\right)^2} \tag{3}$$

The calculation formulas of variation coefficient V_j and weight W_j of each index are shown in Formulas (4) and (5):

$$V_j = \frac{S_j}{\overline{y}_j} \tag{4}$$

$$W_j = \frac{V_j}{\sum_{j=1}^{m} V_j} \tag{5}$$

By applying the double variation coefficient weight assignment method, the corresponding calculation of variation coefficient weights was carried out, and the weights of

each attribute were obtained; By combining the attribute values of the visitor's object role, the weighted permission values for visitors to access electronic financial management data can be obtained.

3.4 Attribute Encryption Secure Access Control Model

After assigning the weights for visitors' access to electronic financial management data, in order to ensure the security of access to electronic financial management data, this paper designs an Attribute Encryption secure access control model Based on Attribute-based Encryption (ABE).

Suppose $A = \{A_1, A_2, ..., A_n\}$ is the set of all attributes, then the object attribute UA is the non-empty subset of A. The attribute set with the number of attributes n can define 2^n attribute subsets in total, so it can identify 2^n users at most.

Access structure AS is a non empty subset of property set $A = \{A_1, A_2, ..., A_n\}$, $AS \subseteq 2^{\{A_1, A_2, ..., A_n\}}$. When the object attribute user appears in the access structure AS, it matches as an authorized user, otherwise it is an unauthorized user.

Assume that G and GT are multiplicative cyclic groups of prime order p, g can be used as the generator of G to bilinear map G. Randomly define M group elements $\{s_1, s_2, ..., s_M\} \in G$ and associate them with the attribute set $A = \{A_1, A_2, ..., A_n\}$, and randomly select two indices $a, b \in Z_p$ to obtain the public key set by the owner of electronic financial management data as follows:

$$PK = \left\{ g, e(g, g)^a, g^b, h_1, h_2, ...h_M \right\} \tag{6}$$

The master key can be calculated as follows:

$$MK = g^a \tag{7}$$

The owner of the electronic financial management data sets a unique ID for the file that needs to be encrypted and stored in the cloud storage center, randomly selects a symmetric key SYK, uses the symmetric key SYK to encrypt the electronic financial management data file, and sets the access structure of the electronic financial management data file. The encrypted ciphertext can be expressed as:

$$CT(t) = Ency \times p(t) \times (PK, \{SYK, K_u, K_w\}, t) \tag{8}$$

where, t represents the timestamp of the encryption process; K_u indicates the write permission corresponding to the signature key, which applies to writable users. Users sign data after performing write operations. K_w indicates the read permission corresponding to the authentication key. It is used to verify the signature result for read-only users.

The owner of electronic financial management data can specify attribute set A_w for each user in the user permission list, and then calculate the private key of the corresponding object attribute user:

$$K_\sigma = keyGen(MK, A_w) \tag{9}$$

After obtaining the object attribute user private key K_σ, encrypt it based on the accessing user's public key PK and send it to the user who needs access.

The owner of electronic financial management data uploads the data file to the cloud for storage, and stores the user permission list of the file share in the cloud, which includes the user ID that the file can access, the valid status of the file, the user list UL of the file share, and the user list of deleted permissions.

3.5 Remote Access Decryption Control

Select any index $r \in Z_p$ for each object attribute user of access control and calculate:

$$D_y = g^a \times H(j)^{rj} \tag{10}$$

$$D'_j = g^{rj} \tag{11}$$

Compose the algorithm key through $D = g^{(\alpha+\beta)/\beta}, \forall j \in S : D_y = \times H(j)^{rj}$ and $D'_j = g^{rj}$.

During the process of remote access decryption control, perform decryption calculations on the ABE algorithm. Convert to recursive algorithm $Decrypt - Node(CT, SK, x)$ as:

$$Decrypt - Node(CT, SK, x) = \frac{e(D_i, C_x)}{e\left(D'_i, C'_x\right)} = e(g, g)^{r(0)} \tag{12}$$

where, x represents the non-leaf node of the decision tree. If S_x represents the set of decision root node children z of any size k_x, it can be stored as F_z through recursive algorithm $Decrypt - Node(CT, SK, z)$, and $F_z \neq \perp$, then it can be calculated:

$$F_x = \prod_{z \in S_x} F_z^{\Delta i, S_x(0)} = e(g, g)^{r(0)} \tag{13}$$

The recursive algorithm is used to determine the key solving process of the ABE algorithm, and the recursive function is used from the root node of the decision tree.

If the attribute set S satisfies the access decision tree T, then:

$$A = Decrypt - Node(CT, SK, r) = e(g, g)^{rs} \tag{14}$$

Thus, the process of remote decryption access control based on ABE algorithm is completed, and remote access control of electronic financial management data based on object attribute matching is realized.

4 Experiment

In order to verify the application performance of the remote access control method of electronic financial management data based on object attribute matching proposed in this paper, a comparative experiment was set up for testing.

4.1 Experimental Environment Settings

Select the financial data of a certain enterprise as the research object, extract the electronic financial management data separately, and import it into a new database. The total amount of existing electronic financial management data is 56.4G. After data cleaning and eliminating duplicate and redundant electronic resource data, there is a remaining 50.0G. Using the Python random sampling algorithm, 80% of the data is used as the training dataset and 20% as the testing dataset. The training dataset is 40.0G, and the testing dataset is 10G. This article implements attribute access control based on dynamic user trust using Matlab tools in the Win10 system environment. The specific parameters of the experimental environment are shown in Table 2.

Table 2. Experimental environment

Project	Parameter
Mobile terminal	ZUK Z2125
CPU	Inter Core i7 2.35Hz
ROM	64GB
RAM	6GB
Android version	6.0.1
Operating system	Ubuntu desktop 11.10 × 64
Open Stack	Essex
Simulation software	MATLAB 2019a
Virtual machine	VMware Workstation 6.5.2

In the experiment, setting the initial credibility of all users to the same value can ensure that the same initial conditions and evaluation criteria are adopted for all users during the application performance verification process to maintain fairness. Meanwhile, for new users, the experimental system may not have enough information to evaluate their level of trust. Therefore, setting their initial credibility to a lower value can reflect their lower level of trust in the system. For certain sensitive operations or critical data, the system may need to exercise more cautious access control. By setting the initial credibility of all users to a lower value, stricter control and review of potential risks can be added. Therefore, in order to simulate a lower initial trust level when verifying application performance and provide a fair and cautious evaluation standard, the initial trust level of all users is set to 0.3, where the proportion of direct credibility is 0.6.

In order to ensure the fairness of experimental testing, the access control method based on RBAC proposed in literature [5] and the access control method based on ABAC proposed in literature [6] are compared in this paper, and the remote access control method based on object attribute matching proposed in this paper is tested together.

The generation time of the private key and the packet loss rate of the remote access control are used as test indicators. The shorter the generation time of the private key,

the lower the packet loss rate of the remote access control, and the better the application performance of the access control method.

4.2 Comparison of Private Key Generation Time

Three different methods were used to calculate the generation time of private keys during access control of electronic financial management data. The comparison results of private key generation time for different methods are shown in Fig. 3.

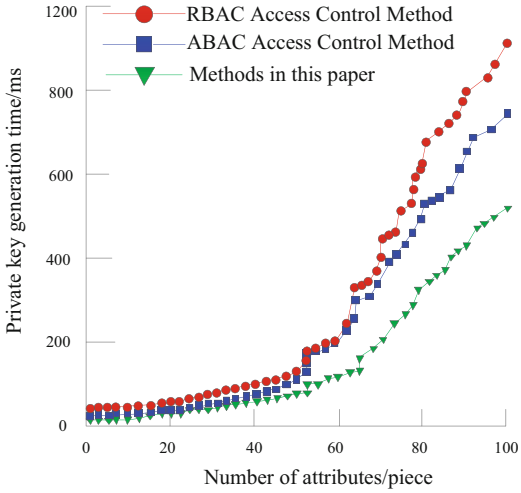

Fig. 3. Comparison of private key generation times

Observing Fig. 3, it can be seen that different methods increase the time for data owners to generate user private keys as the number of attributes changes, and the time for private key generation shows an increasing trend as the number of attributes increases. The average private key generation time of RBAC-based access control method and Abac-based access control method is about 298ms and 262ms, while the average private key generation time of the proposed method is about 205ms. When the number of attributes is less than 50, the performance of the comparison method has little difference, but when the number of attributes is more than 50, the private key generation time starts to show a significant gap. When the number of attributes reaches 60, the access control methods of RBAC and ABAC show a very obvious upward trend. Although the private key generation time of this method is gradually increasing, it is always lower than the two methods compared, and the private key generation time is shorter, indicating that this method has good application performance.

4.3 Packet Loss Rate for Remote Control

Three different methods were used to calculate the packet loss rate of remote control when accessing electronic financial management data. The comparison results of remote control packet loss rates using different methods are shown in Fig. 4.

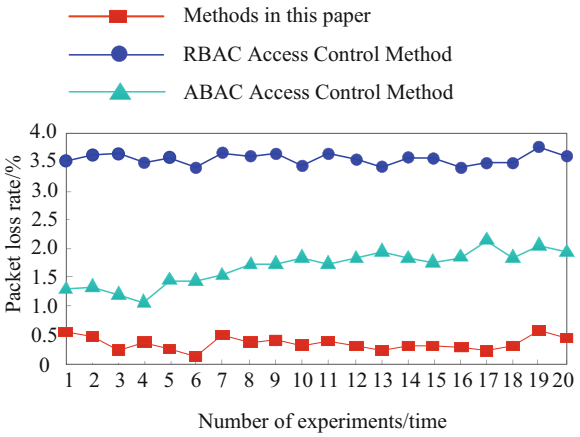

Fig. 4. Comparison of packet loss rates for remote control

Observing Fig. 4, it can be seen that after 20 experimental tests, the packet loss rate of remote control when accessing electronic financial management data based on RBAC is between 3.2% and 3.7%, and that of remote control when accessing electronic financial management data based on ABAC is between 1.0% and 2.0%. However, the packet loss rate of remote control is between 0.2% and 0.7% when accessing electronic financial management data, which is always lower than 1.0%, indicating that the access control security of the proposed method is high and it has good application performance.

5 Conclusion

Access control of data can help data owners implement coarse-grained and fine-grained access control policies, ensuring that sensitive data is only accessed and processed by authorized personnel, and avoiding the risk of malicious attacks or data leakage. In response to the shortcomings of existing remote access control methods for data, this article proposes a remote access control method for electronic financial management data based on object attribute matching.

(1) Determine the object attributes for accessing electronic financial management data, set the access permission category for electronic financial management data files, and match the object attributes of external access control; Assign weights to electronic financial management data, design a secure access control model based on attribute encryption, and use recursive algorithms to decrypt and control remote access, achieving remote access control of electronic financial management data.
(2) Through experiments, it has been proven that the average private key generation time of the proposed method for accessing electronic financial management data is about 205ms, and the packet loss rate of remote control is always below 1.0%, indicating good application performance.

Acknowledgement. 1. 2022 Annual Project of the "14th Five-Year Plan" Education and Science Planning of Shaanxi Province: Research on the ideological situation of university students and their guidance path in the era of convergent media (SGH22Y1721).

2. Research Projects of Xi'an Jiaotong University City College in 2021: Research on accounting information quality improvement methods based on blockchain technology (2021X29).

References

1. Wang, J., Zhang, W.: Attribute and RBAC based access control model and algorithm research. J. Chin. Comput. Syst. **43**(07), 1523–1528 (2022)
2. Liu, W., Sheng, C., She, W., et al.: Classified and hierarchical attribute access control method based on smart contract. Appl. Res. Comput. **39**(05), 1313–1318 (2022)
3. Pan, R., Wang, G., Huang, H.: Attribute access control based on dynamic user trust in cloud computing. Comput. Sci. **48**(05), 313–319 (2021)
4. Wei, D., Sheng, B., Xiang, W., et al.: Access control model in PDM system based on role and attribute. Mach. Des. Manuf. **12**, 259–263 (2019)
5. He, S., Ou, B., Liao, X.: Role matching access control model for distributed workflow. Comput. Sci. **45**(07), 129–134 (2018)
6. Shao, R., Tian, X.: ABAC access control scheme based on MQTT protocol in smart grid. Appl. Res. Comput. **39**(11), 3436–3443 (2022)
7. Zhou, C., Ren, Z.: Research of access control model combined attribute with role. J. Chin. Comput. Syst. **39**(04), 782–786 (2018)
8. Ge, L., Hu, Y., Zhang, G., et al.: Reverse hybrid access control scheme based on object attribute matching in cloud computing environment. J. Comput. Appl. **41**(06), 1604–1610 (2021)
9. Guo, X., Wang, Y., Feng, T., et al.: Blockchain-based role-delegation access control for industrial control system. Comput. Sci. **48**(09), 306–316 (2021)
10. Yu, B., Tai, X., Ma, Z.: Study on attribute and trust-based RBAC model in cloud computing. Comput. Eng. Appl. **56**(09), 84–92 (2020)