Efficient Hierarchical Key Management Scheme for VR/AR Database Systems

Tsung-Chih Hsiao[1], Yu-Min Huang[2], Yu-Fang Chung[3], Tzer-Long Chen[4], and Tzer-Shyong Chen[5]

(Corresponding author: Tzer-Shyong Chen)

School of Arts, Southeast University, Nanjing, China[1]
Department of Statistics, Tunghai University, Taiwan[2]
Department of Electrical Engineering, Tunghai University, Taiwan[3]
Department of Information Technology, Ling Tung University,Taichung, Taiwan[4]
Department of Information Management, Tunghai University, Taiwan[5]
(Email: arden@thu.edu.tw)

(Received Feb. 26, 2018; Revised and Accepted Aug. 13, 2018; First Online Mar. 9, 2019)

Abstract

With the growth of Virtual Reality (VR) and Augmented Reality (AR) in technologies such as artificial intelligence, wireless, 5G, big data, massive compute, industrial 4.0 and virtual stores. This paper improved the secure mechanism which existed some shortcomings. In order to accomplish the decentralized environment access control, it also proposed another new mechanism to achieve the requirements on the nonspecific internet. Besides, considering the security on storing and controlling and the use of administrative privileges of the VR and ARclouds is necessary. With the new mechanism, the problems such as mobile security or acting calculation which derived from VR and AR could be solved. This new research achieves a better circumstance. Developer staff's responsibility can be allocated; the systems can be compatibly integrated; on the other hand, the users' privacy of personal information can be strictly protected.

Keywords: Augmented Reality; Database System; Mobile Security; Privacy; Virtual Reality

1 Introduction

For the VR/AR data in the Internet standardization needs and standards system, research data security standards. Development of general requirements such as general requirements, architecture, testing and evaluation; development of common standards such as Internet and digital interconnection interface, logo resolution, data internet platform and security.The updating of VR/AR system and the insurance system, specifications of the Developer codes and information have several major problems. The consistency of the coding system and the data exchange format are not uniform and the expression ability in the VR/AR information system is quite lacking, etc. Under development of applicable VR/AR information, standards and practical application in the market, VR/AR information system needs to face the problem.

According to the number of VR/AR users, network size and other indicators, VR/AR user data security has become on of the the world's largest issue [6, 15].VR/AR information system equips a data system that is called VR/AR database system. Database is a set of related data collection, and the operation of the database must rely on the Database Management System, DBMS, to operate [5]. The database system is a program that controls the classification of the database and the access to the data [12]. According to the VR/AR information system, the transmitting of VR/AR information or related information, will inevitably use the network. Based on the problems of user's privacy, the developer enterprise's internal and external networks must be comprehensively planned. User's demand is divided into the following points: response, availability, quality, adaptability, security, affordability, expected growth. However, the safety of electronic VR/AR information has also become an important issue, especially for the user's access rights and in different time-range norms. We attempt to utilize mathematical methods to go through the data encryption and decryption which can strictly protect user's VR/AR information [1, 7].

DBMS can be divided into three types – hierarchical, network, relational [2]. The application of this information management system is widely used for relational purposes; however, due to the system used in developer enterprises rely on each other, the system will reject those people who attempt to get access to the user's information.

The feature of blockchain technologies may bring us more reliable and convenient services [9]. In a traditional public-key encryption, the sender has to authenticate that the invoked public key is the legitimate public key for the intended receiver [10].Therefore, in this paper, we propose an integrated hierarchical access mechanism and the characteristics of the database system. By storing the decryption key in the Lagrange interpolation polynomial method, the VR/AR confidential information and users' privacy can be effectively protected [8]. A lot of related works have been proposed to solve access control problems [3,4,11,13,14].

2 Proposed Work

2.1 VR/AR Database Integration of VR/AR Systems

VR/AR systems contain a lot of information in the database, such as VR/AR records. As a result, VR/AR hardware and software communication are regulated. Due to different systems and equipments in different companies, leads to various incompatibilities between VR/AR devices and platforms. The Application Programming Interface standard describes how the VR/AR application or game engine renders its content and receives the data. If both of these core elements are standardized across all VR/AR hardware and software products, there will be an explosion in industry adoption and innovation.DBMS is mainly responsible for processing all data storage and retrieval operations. It can also modify data integration, data consistency check rules, controlling single or multi user's authorization, and data protection, etc. These are one part of the operation of the VR/AR system. For those people who intent to obtain information or even reveal other user's information, the system will cause compatibility obstacles to make the hackers unsuccessfully retrieve the user's information.

In order to make the system manager more convenient access to user information, we seek for access keys to secure confidential files while considering the safety issues in the transmission process. Therefore, this research method through the public encryption system and Lagrange interpolation of VR/AR data encryption protection, through the key authentication management center issued legal authority user decryption key, allowing users to access to the decryption key secret documents, strict management of the user data.

2.2 An Improved Access Scheme

Our goal is to construct the key allowing a server to access a particular document. We generalize the decryption polynomial $F_{DK_j}(x)$ subject to the following criterion (Table 1).

$$F_{DK_j}(x) = \begin{cases} DK_j, & \text{if server } S_i \text{ has permission} \\ & \quad \text{to access } j \text{ document} \\ C, & \text{Otherwise} \end{cases} \qquad (1)$$

for $C \neq DK_j$.

We aim to enhance the security over the decryption key to avoid potential exploration of information revealed by a third party.

2.3 Key Production

The decryption key can be generated through the following steps.

Step 1: Select large prime numbers p and q in random as the roots of finite field $GF(p)$. Number g and p remain public.

Step 2: Each confidential document will use non-repetitive decryption key DK_j, $j = 1, 2, \cdots, n$ with n denoting the number of documents.

Step 3: Choose non-repetitive secret key K_i, $i = 1, 2, \cdots, m$, where m is the number of servers which are about to visit confidential documents.

Step 4: The mobile agent owner uses a set of interpolation polynomial at with ID_j represents the number of DK_j. If $DK_i \leq S_i$, S_i has permission to get the decryption key DK_j. We construct $F_{DK_j}(x)$ as below.

$$\begin{aligned} F_{DK_j}(x) &= x + DK_j - [\sum_{DK_j \leq S_i} x_{ij} l_{ij}(x) \\ &\quad + \prod_{DK_j \leq S_i} a(l_{ij}(x))R], \end{aligned} \qquad (2)$$

where $l_{ij}(x)$ is the Lagrange interpolation polynomial formulated as:

$$\begin{aligned} l_{ij} &= \prod_{t=1, t\neq i}^{m} (\frac{x - x_{1j}}{x_{ij} - x_{1j}}) \cdots (\frac{x - x_{i-1,j}}{x_{ij} - x_{i-1,j}})(\frac{x - x_{i+1,j}}{x_{ij} - x_{i+1,j}}) \\ &\quad \cdots (\frac{x - x_{mj}}{x_{ij} - x_{mj}}) \end{aligned} \qquad (3)$$

We have Hash Function noted as:

$$a(l_{ij}(x)) = \begin{cases} l_{ij}(x) - 1, & \text{if } l_{ij}(x) = 1 \\ 1, & \text{Otherwise} \end{cases} \qquad (4)$$

and R stands as a random real number.

2.4 Key Derivation

The decryption polynomial $F_{DK_j}(x)$ will derivate the decryption key through access permission from section above.

1) Server S_i providing a decription key DK_j for which the far-end server will be able to access the j document.

2) Server S_i substitutes its secret key K_i and decryption key ID_j for the public decryption polynomial equation $F_{DK_j}(x)$ to get DK_j. This access can be carried through the following derivation.

Table 1: Parameters for generating the decryption process

Symbols	Definition
CA	The key authentication management center
S_i	Server (System User)
ID_t	Number of confidential documents
K_i	The private key corresponding to each legitimate user
DK_t	Corresponds to the IDt‘s decryption key
$F_{DK_t}(x_i, t)$	Public decryption polynomial for retrieving decryption key

If $DK_i \leq S_i$, the secret key K_i provides x_{ij} and the Lagrange interpolation polynomial turns to be

$$l_{ij}(x_{ij}) = \prod_{t=1, t\neq i}^{m} (\frac{x - x_{tj}}{x_{ij} - x_{tj}}) = 1 \tag{5}$$

while the same x_{ij} we have $l_{ij}(x_{ij}) = 0$, for $i' \neq i$ or $j' \neq j$. This gives us the Hash Function as shown below:

$$a(l_{ij}(x_{ij})) = \begin{cases} l_{ij}(x_{ij}) - 1, & \text{for } i, j \\ 1, & \text{for } i' \neq i \text{ or } j' \neq j. \end{cases} \tag{6}$$

Thus, we have Equation (7):

$$\begin{aligned} \prod_{DK_j \leq S_i} a(l_{ij}(x_{ij})) &= 1 \cdots 1[l_{ij}(x_{ij}) - 1]1 \cdots 1 \\ &= 0. \end{aligned} \tag{7}$$

$$\sum_{DK_j \leq S_i} x_{ij} l_{ij}(x_{ij}) = x_{ij}. \tag{8}$$

Finally we put Equations (7), (8) into decryption polynomial in order to get decryption key DK_j:

$$F_{DK_j}(x_{ij}) = x_{ij} + DK_{ij} - x_{ij} = DK_j. \tag{9}$$

If $l_{ij} \neq 0, 1$, then we have

$$F_{DK_j}(x) = x + DK_j - [\sum_{DK_j \leq S_i} x_{ij} l_{ij}(x) + R]$$

Which means it would not be the desired decryption key DK_j either.

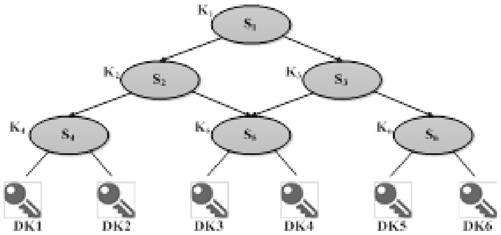

Figure 1: Access control architecture diagram for mobile agents

3 Example

According to the hypothetical hierarchical scheme (Figure 1), we assume that server S_6 has permission to access document 5 and 6. We demonstrate how the decryption process works to give the access key to the server. Suppose that we want to provide the decryption key to document 1, 3, 6 for server S_6, we have the following calculation shown below if S_6 uses input key x_{66}.

$$\begin{aligned} l_{16}(x_{66}) &= (\frac{x_{66} - x_{26}}{x_{16} - x_{26}})(\frac{x_{66} - x_{36}}{x_{16} - x_{36}})(\frac{x_{66} - x_{46}}{x_{16} - x_{46}}) \\ &\quad (\frac{x_{66} - x_{56}}{x_{16} - x_{56}})(\frac{x_{66} - x_{66}}{x_{16} - x_{66}}) = 0 \end{aligned} \tag{10}$$

$$\begin{aligned} l_{36}(x_{66}) &= (\frac{x_{66} - x_{16}}{x_{36} - x_{16}})(\frac{x_{66} - x_{26}}{x_{36} - x_{36}})(\frac{x_{66} - x_{46}}{x_{36} - x_{46}}) \\ &\quad (\frac{x_{66} - x_{56}}{x_{36} - x_{56}})(\frac{x_{66} - x_{66}}{x_{36} - x_{66}}) = 0 \end{aligned} \tag{11}$$

$$\begin{aligned} l_{66}(x_{66}) &= (\frac{x_{66} - x_{16}}{x_{66} - x_{16}})(\frac{x_{66} - x_{26}}{x_{66} - x_{26}})(\frac{x_{66} - x_{36}}{x_{66} - x_{36}}) \\ &\quad (\frac{x_{66} - x_{46}}{x_{66} - x_{46}})(\frac{x_{66} - x_{56}}{x_{66} - x_{56}}) = 1. \end{aligned} \tag{12}$$

We also obtain values of Hash Function with $(l_{16}(x_{66})) = 1$, $a(l_{36}(x_{66})) = 1$, $a(l_{66}(x_{66})) = 0$ since Lagrange interpolation polynomials have been evaluated from Equations (10), (11), (12). Therefore, we can retrieve decryption key through decryption polynomial shown below:

$$F_{DK_6}(x_{66}) = x_66 + DK_6 - [x_{66} + 0] = DK_6. \tag{13}$$

For the case that the server S6 uses a input key such as $x_* \neq x_{66}$ or $x_* \neq$ any linear combination of key x_{11}, x_{22}, x_{33}, $\cdots$ and so on, then we have:

$$\begin{aligned} l_{16}(x_*) &= (\frac{x_* - x_{26}}{x_{16} - x_{26}})(\frac{x_* - x_{36}}{x_{16} - x_{36}})(\frac{x_* - x_{46}}{x_{16} - x_{46}}) \\ &\quad (\frac{x_* - x_{56}}{x_{16} - x_{56}})(\frac{x_* - x_{66}}{x_{16} - x_{66}}) = c_1, c_1 \neq 0, 1 \end{aligned} \tag{14}$$

$$\begin{aligned} l_{36}(x_*) &= (\frac{x_* - x_{16}}{x_{36} - x_{16}})(\frac{x_* - x_{26}}{x_{36} - x_{36}})(\frac{x_* - x_{46}}{x_{36} - x_{46}}) \\ &\quad (\frac{x_* - x_{56}}{x_{36} - x_{56}})(\frac{x_* - x_{66}}{x_{36} - x_{66}}) = c_2, c_2 \neq 0, 1 \end{aligned} \tag{15}$$

$$\begin{aligned} l_{66}(x_*) &= (\frac{x_* - x_{16}}{x_{66} - x_{16}})(\frac{x_* - x_{26}}{x_{66} - x_{26}})(\frac{x_* - x_{36}}{x_{66} - x_{36}}) \\ &\quad (\frac{x_* - x_{46}}{x_{66} - x_{46}})(\frac{x_* - x_{56}}{x_{66} - x_{56}}) = c_3, c_3 \neq 0, 1. \end{aligned} \tag{16}$$

Then we get the decryption equation shown below:

$$\begin{aligned} F_{DK_6}(x_*) &= x_* + DK_6 - [x_*(c_1 + c_2 + c_3 + R)] \\ &\neq DK_6. \end{aligned} \tag{17}$$

Which means the server fails to get the decryption key, that is, the confidential documents have been protected from illegal attempts.

Other failure case could be the one that we suppose the server S_6 uses input key x_{56}, then we calculate Lagrange interpolation first , the results shown below:

$$\begin{aligned} l_{16}(x_{56}) &= (\frac{x_{56} - x_{26}}{x_{16} - x_{26}})(\frac{x_{56} - x_{36}}{x_{16} - x_{36}})(\frac{x_{56} - x_{46}}{x_{16} - x_{46}}) \\ &\quad (\frac{x_{56} - x_{56}}{x_{16} - x_{56}})(\frac{x_{56} - x_{66}}{x_{16} - x_{66}}) = 0 \end{aligned} \tag{18}$$

$$\begin{aligned} l_{36}(x_{56}) &= (\frac{x_{56} - x_{16}}{x_{36} - x_{16}})(\frac{x_{56} - x_{26}}{x_{36} - x_{36}})(\frac{x_{56} - x_{46}}{x_{36} - x_{46}}) \\ &\quad (\frac{x_{56} - x_{56}}{x_{36} - x_{56}})(\frac{x_{56} - x_{66}}{x_{36} - x_{66}}) = 0 \end{aligned} \tag{19}$$

$$\begin{aligned} l_{66}(x_{56}) &= (\frac{x_{56} - x_{16}}{x_{66} - x_{16}})(\frac{x_{56} - x_{26}}{x_{66} - x_{26}})(\frac{x_{56} - x_{36}}{x_{66} - x_{36}}) \\ &\quad (\frac{x_{56} - x_{46}}{x_{66} - x_{46}})(\frac{x_{56} - x_{56}}{x_{66} - x_{56}}) = 0. \end{aligned} \tag{20}$$

Hence, we have decryption polynomial equation calculated below:

$$F_{DK_6}(x_{56}) = x_{56} + DK_6 - (x_{56} \times 0 + R) \neq DK_6. \tag{21}$$

Eventually, we know that the server uses the wrong input key x_{56}, which causes the decryption polynomial $F_{DK_j}(x)$ to generate the false decryption key that can't open the confidential documents at all.

4 Analysis of Security

We would discuss from the viewpoint of attackers to compromise the proposed scheme to confirm the method is secure. The attackerssteals from outside.They hacks valuable information in order to accumulate money. This situation could result in the divulgence of confidential information and damages. Accordingly, this becomes a serious issue in the process of security analyses. Regarding external attack, attackers with the knowledge of public parameters are not able to obtain any decryption key DK_t and, consequently, they are not able to obtain any confidential file. If the external attackers wish to extract the secret key SK_i from the interpolation function parameters $x_{ij} = ID_j || g^{SK_i} (\mathrm{mod} p)$, then they have to solve the Discrete logarithm problem; which is known to be computationally infeasible since p is a large prime.

The reversed attack is defined as the user with lower authority intends to access the higher level. If a user successfully carries out a reversed attack on a user who has higher authority, then the attacker could illegally obtain the secret key to access to the confidential documents. After hacking the information successfully, the attackers may tend to sell it which would result in loss to the organization. It is thus important to prevent reversed attack.

5 Conclusions

The biggest challenge for VR/AR development is the security of privacy user data. This paper introduces Virtual Integrated VR/AR-information Systems. This concept is used to achieve dependence and provide a safe environment for enterprise institutes to exchange information online based on user's right management mechanism to access the confidential documents, that manager can efficiently achieve the user's complete VR/AR information. However, there is a risk of data transfer. Theft or tampering of data on the Internet so that the user or server permission to add a hierarchical access control, to ensure that patients in the premise of data confidentiality and safety, effective and safe for authorized manager to use, not has been authorized users, to ensure user privacy will not be violated.

Acknowledgments

This study was supported by the introduction of talents Southeast University Scientific Research Projects (Nos. 3213048201).

References

[1] E. Bierman, T. Pretoria and E. Cloete, "Classification of malicious host threatsin mobile agent computing," in *Proceedings of the Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on Enablement Through Technology*, no. 5, pp. 34–49, 2002.

[2] A. Castiglione, *et al.*, "Hierarchical and shared access control," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 4, pp. 850–865, 2016.

[3] A. Castiglione, A. D. Santis, B. Masucci, F. Palmieri, A. Castiglione and X. Y. Huang, "Cryptographic hierarchical access control for dynamic structures," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 10, pp. 2349–2364, Oct. 2016.

[4] W. Y. Chao, C. Y. Tsai and M. S. Hwang, "An improved key-management scheme for hierarchical access control," *International Journal of Network Security*, vol. 19, no. 4, pp. 639–643, July 2017.

[5] V. El-khoury, N. Bennani and A. M. Ouksel, "Distributed key management in dynamic outsourced databases: A trie-based approach," in *First International Conference on Advances in Databases, Knowledge, and Data Applications*, Gosier, pp. 56–61, 2009.

[6] J. Kasurinen, "Usability issues of virtual reality learning simulator in healthcare and cybersecurity," *Procedia Computer Science*, vol. 119, pp. 341–349, 2017.

[7] K. C. Laudon and J. P. Laudon, *Management Information Systems*, Pearson, Chapter 6: Information systems Organizations and Strategy, pp.143, 2011.

[8] H. Y. Lin, D. J. Pan, X. X. Zhao and Z. R. Qiu, "A rapid and efficient pre-deployment key scheme for secure data transmissions in sensor networks using lagrange interpolation polynomial," in *International Conference on Information Security and Assurance (ISA'08)*, pp. 261–265, 2008.

[9] I. C. Lin and T. C. Liao, "A survey of blockchain security issues and challenges," *International Journal of Network Security*, vol. 19, no. 5, pp. 653–659, Sept. 2017.

[10] L. Liu, W. Kong, Z. Cao, J. Wang, "Analysis of one certificateless encryption for secure data sharing in public clouds," *International Journal of Electronics and Information Engineering*, vol. 6, no. 2, pp. 110–115, June 2017.

[11] J. W. Lo, M. S. Hwang, C. H. Liu, "A simple key assignment for access control based on polynomial," *The Arabian Journal for Science and Engineering*, vol. 38, no. 6, pp. 1397–1403, June 2013.

[12] Z. M. Ozsoyoglu and J. Wang, "A keying method for a nested relational database management system," in *Eighth International Conference on Data Engineering*, Tempe, AZ, pp. 438–446, 1992.

[13] T. H. Sun and M. S. Hwang, "A hierarchical data access and key management in cloud computing," *ICIC Express Letters*, vol. 6, no. 2, pp. 569–574, 2012.

[14] S. H Tang, X. Y. Li, X. Y. Huang, Y. Xiang and L. L. Xu, "Achieving simple, secure and efficient hierarchical access control in cloud computing," *IEEE Transactions on Computers*, vol. 65, no. 7, pp. 2325–2331, July 2016.

[15] X. C. Zhang and X. L. Zhao, "Based on virtual reality technology security intelligent wireless network resources dynamic allocation method research," *Science Technology and Engineering*, vol. 15, pp. 283–288, 2017.

Biography

Tsung-Chih Hsiao received the Ph.D. in the Department of Computer Science and Engineering, National Chung Hsing University, Taiwan. He is currently an associate professor in the School of Arts at Southeast University, China. Research fields include Information Security, Cryptography, and Network Security.

Yu-Min Huang received the Ph.D. in the Department of Statistics at the University of Minnesota Twin Cities, United States. She is currently an assistant professor in the Department of Statistics at the Tunghai University, Taiwan. Research fields include Statistical Inference, Multivariate Statistics, and Statistical Computing.

Yu-Fang Chung received a B.A. degree in English Language, Literature and Linguistics from Providence University in 1994, an M.S. degree from Dayeh University in 2003, and a Ph.D. degree from National Taiwan University in 2007, both in Computer Science, Taiwan. She is currently a professor in the Departments of Electronic Engineering and Information Management at Tunghai University, doing research, i.e., Information Security and Cryptography.

Tzer-Long Chen received the Ph.D. in the Department of Information Management, National Taiwan University, Taiwan. He is currently an assistant professor in the Department of Information Technology at Lingtung University, Taiwan. Research fields include Information Security, Cryptography, and Network Security.

Tzer-Shyong Chen received the Ph.D. in the Department of Electrical Engineering (Computer Science) at National Taiwan University, Taiwan. He is currently a professor in the Department of Information Management at Tunghai University, Taiwan. Research fields include Information Security, Cryptography, and Network Security.