International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

ELSEVIER SSRN

IJIEMR Transactions, online available on 20th Dec 2019. Link :http://www.ijiemr.org/downloads.php?vol=Volume-08&issue=ISSUE-12

Title CAPABLE DYNAMIC RECOGNITION AND RETREAT IN CLOUD COMPUTING

Volume 08, Issue 12, Pages: 153–156.

Paper Authors

RUSHIKESH SHRIDHAR MIRAJKAR, P.SUDHAKAR RAO

Nishitha College of Engineering & Technology, Hyderabad, T.S, India

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

CAPABLE DYNAMIC RECOGNITION AND RETREAT IN CLOUD COMPUTING

RUSHIKESH SHRIDHAR MIRAJKAR[1], P.SUDHAKAR RAO[2]

[1]M.Tech Student, Dept of CSE, Nishitha College of Engineering & Technology, Hyderabad, T.S, India

[2]Asst Professor, Dept of CSE, Nishitha College of Engineering & Technology, Hyderabad, T.S, India

ABSTRACT:

Biological identification has become more popular in recent years. With the development of cloud computing, database owners are motivated to outsource the large amount of biometric data and identification tasks to the cloud to get rid of expensive storage and account costs, which however bring threats Potential for user privacy. In this document, we suggest a plan to outsource vital identification and maintain privacy. Specifically, biometric data is encrypted and outsourced to a cloud server. To implement a biometric definition, the database owner encrypts the query data and sends it to the cloud. The cloud performs identification operations through the encrypted database and returns the result to the owner of the database. A thorough security analysis indicates that the proposed scheme is safe even if attackers can develop identification requests and collude with the cloud. Compared to the previous protocols, the experimental results show that the proposed scheme works best in the preparation and selection procedures.

Keywords: biometric identification; data outsourcing; privacy-preserving; cloud computing

1. INTRODUCTION:

The biometric identification process has aroused increasing interest as it provides a promising method to identify users. Compared to traditional passwords and identification card authentication methods, biometric identification is more reliable and convenient [1]. In addition, biometric recognition has been widely applied in many areas using biometric features such as fingerprint [2], iris [3] and facial patterns [4], which can be obtained from different sensors [5]. In a biometric identification system, the owner of a database, such as the FBI responsible for managing the national fingerprint database, may want to outsource the massive dynamic data data on the cloud server (such as Amazon) to Get rid of expensive storage and account costs. However, to maintain the privacy of vital data, vital data must be encrypted before outsourcing. When an FBI partner (for example, the police station) wants to authenticate the identity of an individual, they turn to the FBI and create an identification query using the individual's vital characteristics (such as fingerprints,

iris, voice patterns, facial patterns , etc.). Then, the FBI encrypts the query and sends it to the cloud to find the exact match. Therefore, the difficult problem is how to design a protocol that provides dynamic, efficient and privacy identification in the cloud. Several identification solutions that maintain privacy have been proposed. However, most of them focus primarily on preserving privacy but ignore efficiency, such as smoothed coding and forgotten schemes based on portability in fingerprint and face recognition, respectively. Due to the performance problems of local devices, these graphics are not effective once the database size is larger than 10 MB, and provides an identification scheme that uses circuit design and text coding techniques to achieve an effective definition of a larger database of up to 1 GB. In addition, a biometric identification system is proposed to maintain privacy. Specifically, they built three modules and designed a specific protocol to achieve the security of a fingerprint function. To improve efficiency, in its scheme, the database owner outsources the identification of the tasks corresponding to the cloud. However, he noted that the protocol could be broken by a collusion attack by a malicious user and the cloud. Wang et al. The Cloud BI-II system that uses random diagonal matrices to achieve identification is suggested. However, his work has proved insecure. In this document, we suggest an efficient and privacy-sensitive biometric identification system that can withstand the collusion attack by users and the cloud. Specifically, our main contributions can be summarized as follows:

• We are studying the biometric identification scheme and showing security deficiencies and vulnerabilities in the context of the proposed Level 3 attack. Specifically, we demonstrate that an attacker can recover his secret keys by colluding with the cloud and then deciphering the vital characteristics of all users .

• We present a new identification system that is effective and maintains privacy. The detailed security analysis shows that the proposed scheme can reach the required level of privacy protection. Specifically, our scheme is safe under the outsourcing identification model and can also withstand the proposed attack.

• Compared to current identification plans, the performance analysis shows that the proposed scheme saves lower computational costs in both preparation and selection procedures.

MODELS AND DESIGN GOALS

Entities participate in the system, including the database owner, users and the cloud. The database owner has a large amount of biometric data (such as fingerprints, iris, sound and face patterns, etc.), which are encrypted and transferred to the cloud for storage. When the user wants to identify himself, a query request is sent to the owner of the database. After receiving the request, the database owner creates the encrypted text for the biometric attribute and then transfers the encrypted text to the cloud for identification. The cloud server determines the best match for the encrypted query and

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

returns the index related to the owner of the database. Finally, the database owner calculates the similarity between the query data and the biometric data associated with the index, and returns the result of the query to the user. In our diagram, we assume that the biometric data has been processed so that its representation can be used to perform the biometric comparison. Without loss of generality, just as we point to fingerprints, we use finger codes to represent fingerprints. More specifically, FingerCode consists of n elements and each element is an integer bit number (usually n = 640 and 1 = 8). Looking at two finger symbols x = [x1, x2, • • •, xn] ey = [y1, y2, • • •, yn], if the Euclidean distance is below the threshold, it is generally considered a good match, Which means that two fingerprints are considered the same person.

DESIGN GOALS

To achieve a practical application, both safety and efficiency are considered in the proposed scheme. To be more specific, the objectives of the proposed design scheme are described below:

Efficiency: the computational costs must be as low as possible both on the owner side of the database and on the user side. For high efficiency, most identification operations must be performed in the cloud.

Security: during the identification process, the privacy of vital data must be protected. The attackers and the semi-honest cloud should not learn anything about confidential information.

SECURITY ANALYSIS OF YUAN AND YU'S SCHEME

First we describe Yuan and Yu diagrams, then we present the security analysis of their diagram. To make the diagram easier to understand, we use to denote multiplication of elements, and we use to denote matrix or vector multiplication.

YUAN AND YU'S SCHEME

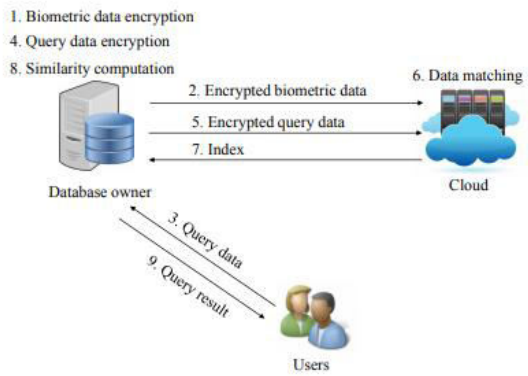
Step 1: The database owner randomly creates (n + 1) x (n + 1) matrix A where H x AT i = 1 and Ai is a row vector in A, 1 ≤ i ≤ (n + 1). Then, the database owner creates a corresponding matrix Di = [AT 1 bi1, AT 2 bi2, • AT n + 1 bi (n + 1)] to hide Bi. After that, the owner of the database performs

Step 2: After performing step 1, the cloud stored many tuples in its C database. When the user requests to determine his identity, he / she expands a binary and then submits the extended query Bi to the database owner. Upon receiving the request from the user, the database owner creates a random matrix (n + 1) x (n + 1) E so that Ei x RT = 1, where Ei is the row vector in array E and 1 ≤ i ≤ (n + 1). The database owner then creates a corresponding matrix Fc = [ET 1bc1, ET 2 bc2, • • • n n + 1 bc (n + 1)] T to hide the FingerCode Bc query. The owner of the database then performs

Step 3: Upon receiving Cf, the cloud begins to search for the best match. Specifically, the pi = Ch x Ci x Cf x Cr is calculated for each encoded biometric database to compare the Euclidean distances between bc and bi. Other details are deleted because they are inappropriate for the safety analysis we will

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

describe.



The biometric identification system is safe if it can resist the α level attack (α ∈ {1,2,3}). Note that if the proposed scheme can resist level 2 and level 3 attacks, this does not mean that the attacker can be a valid user and monitor some incorrect texts of the biometric database simultaneously. This sophisticated attack is very powerful and there are no effective means designed to defend against this type of attack [14]. In this paper, we focus on collusion attack between a malicious user and the cloud server. The relationship between dynamic database texts and encrypted texts is unknown to the attacker, and is similar to the attack model

CONCLUSION

We proposed a new identification system that maintains privacy in the cloud. For efficiency and safe requirements, we designed a new encryption algorithm and cloud authentication certificate. Detailed analysis shows that it is able to resist potential attacks. Besides, through performance appraisals, we have shown that the proposed scheme meets the need for efficiency well.

REFERENCES:

[1] A. Jain, L. Hong and S. Pankanti, "Biometric identification," Communications of the ACM, vol. 43, no. 2, pp. 90-98, 2000.

[2] R. Allen, P. Sankar and S. Prabhakar, "Fingerprint identification technology," Biometric Systems, pp. 22-61, 2005.

[3] J. de Mira, H. Neto, E. Neves, et al., "Biometric-oriented Iris Identification Based on Mathematical Morphology," Journal of Signal Processing Systems, vol. 80, no. 2, pp. 181-195, 2015.

[4] S. Romdhani, V. Blanz and T. Vetter, "Face identification by fitting a 3d morphable model using linear shape and texture error functions," in European Conference on Computer Vision, pp. 3-19, 2002.

[5] Y. Xiao, V. Rayi, B. Sun, X. Du, F. Hu, and M. Galloway, "A survey of key management schemes in wireless sensor networks," Journal of Computer Communications, vol. 30, no. 11-12, pp. 2314-2341, 2007.