Mobile Database Model Based on Secret Sharing Protocol

Juan Ran
School of Information Engineering
Zhengzhou University
Zhengzhou City, P. R. China
ieranjuan@163.com

Xiaoyu Li
School of Information Engineering
Zhengzhou University
Zhengzhou City, P. R. China
iexyli@zzu.edu.cn

Abstract—Considering the limited resource and capability, a mobile database model based on secret sharing protocol is proposed. The system achieves the mechanism of the least privilege with the use of secret sharing protocol, which guarantees that only the mobile client can get both the key and the cipher text. The security level of the system is improved for original database can be recovered with the involvement of more than k servers. Even if some storage servers break down, it won't affect the data access from the mobile clients, which improves the robustness of the mobile database system. The experiment results show that the model is feasible with good performance and practical value.

Keywords-mobile database; secret sharing protocol; AES algorithm; security; robustness.

I. INTRODUCTION

With the development of mobile internet and the popularization of mobile device, people can access the data on the Internet whenever and wherever possible. The 30th Statistics Report on Internet Development in China shows that the utilization rate of mobile phones to surf the Internet is 83.4% which first exceeds that of PC (80.9%). But databases in mobile environment face a group of restrictions, such as limited computing power, limited energy, limited memory space, limited capacity of channel and low robustness of mobile terminals. All these problems make that traditional database technology is not suitable to be applied in mobile environment. So as a technology which is more fit to be applied in mobile internet, mobile database becomes more and more popular and important.

Mobile database is a kind of distributed database which supports mobile computing environment. It has been one of the most important fields in the research of distributed database with broad prospects to be applied into mobile internet service [1-3]. Secret sharing protocol is encryption technology which splits secret information into several parts and stores them respectively. It can prevent secret information from being centrally stored so as to diversify risks and defeat attack. In a (k, n) threshold secret sharing protocol in which k<n, the original information is encrypted and split into n parts. If one collects m parts (m≥k), he can recover the original information. Or the original information can' t be recovered.

This paper provides a mobile database model based on the secret sharing protocol. First we encrypt the database by AES algorithm [4] and produce n copy of the encrypted database. Then the key is divided into n parts (named key shadow) by (k, n) Shamir threshold secret sharing protocol [5] in which every part is attached with one copy of the database. Next the n (shadow, copy) pairs are distributed to n mobile terminals in which a terminal is named a storage server. When a user wants to access the database, he must get at least k key shadows to recover the key and decrypt the encrypted database. This model can achieve higher robustness and higher security than traditional mobile database system. Experiment results show that the model is feasible and it can achieve good performance and practical value.

II. BASIC IDEA

AES cryptographic algorithm is a high-level standard of encryption algorithm which is also called Rijindael algorithm. It's a block encryption standard used by American government which has replaced insecure DES algorithm and slow 3-DES algorithm. AES algorithm is an iterative block symmetrical cipher scheme which has been applied in cryptosystem all over the world.

Shamir threshold secret sharing protocol [5-9] is a (k, n) threshold secret sharing protocol which is mostly applied in practice. It can achieve the mechanism of least privilege, in other words, every user in this cryptosystem only hold not all privileges but the least set of privileges. So it can greatly reduce the risk as possible.

The mobile database model based on the secret sharing model is the integration of AES algorithm, Shamir secret sharing protocol and mobile database. It can be showed as the following Fig .1.

There are four roles in the mobile database model including mobile client, encryption server, storage server and recover server.

(1) mobile client: a mobile terminal which wants to access the database.
(2) encryption server: a mobile terminal or a computer in the fixed network.
(3) storage server: a mobile terminal which keeps the encrypted database.
(4) recover server: a mobile terminal which is chosen to recover the key and decryption the database. It's also the database server which serves for the mobile clients.

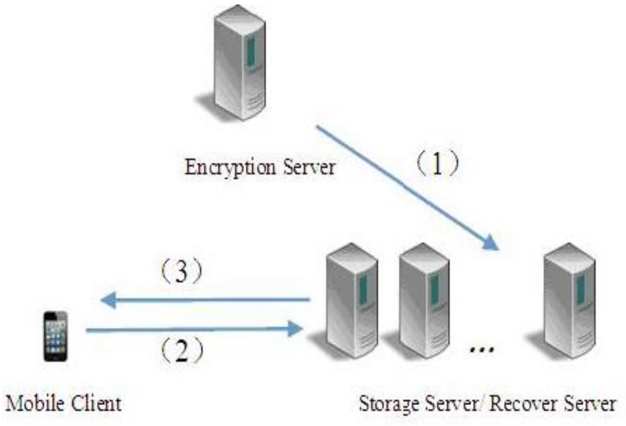

Figure 1. Data access in the mobile database model

We assume that first the encryption server encrypts the original database by AES algorithm with a 128-bit key to produce n copies of encrypted databases. Then the encryption server performs Shamir (k, n) secret sharing protocol on the key. So it gets n key shadows. Next the encryption server distributes the n (shadow, copy) pairs to n storage servers. When a mobile client wants to access the database, it chooses k storage servers out. It's easy to find that the k storage servers can recover the key by their k key shadows. So the original database can be recovered from the encrypted database on any one of the k storage servers, too. Now the mobile client can access the original database. So we can design a mobile database model based on this idea.

III. Mobile Database Model Based on the Secret Sharing Protocol

The mechanism of our mobile database model based on the secret sharing protocol is described as the following steps.

Step 1: the encryption server chooses a 128-bit key to encrypt the original database by AES algorithm to produce n copies of the encrypted database. Then it splits the key into n key shadows by Shamir (k, n) threshold secret sharing protocol. Finally the encryption server sends the n (shadows, copy) pairs to n terminals which it has chosen out as the n storage servers.

Step 2: when a mobile client wants to access the database, it first chooses k storage servers out. Then the mobile client chooses one storage server as the recover server by a load balancing algorithm in which the storage server with more memory space and more computing power gets the prior [10]. Next the mobile client asks the left k-1 storage server to send their key shadows to the recover server.

Step 3: Now the recover server gets k key shadows after it receives the key shadows from the left k-1 storage server. It can recover the key by Lagrange interpolation method easily. Then the recover server decrypts the encrypted database by AES algorithm with the key. Finally the recover server gets the original database. It becomes the database server for the mobile client.

Step 4: The mobile client accesses the database on the recover server.

Step 5: After the mobile client finishes its data access, the recover server deletes the original database and the key. So it turns back into a common storage server.

IV. The Advantages of the Mobile Database Model Based on the Secret Sharing Protocol

This mobile database model based on the secret sharing protocol can show several important advantages relative to the previous mobile database model.

(1) If an illegal user wants to access the database, he must get at least k storage server's permissions which is much difficult than cheating only one database server in traditional mobile database model. So our model can achieve high security:

(2) A mobile client only needs to choose k storage servers at random when it wants to access the database. If one or a few storage servers break down, mobile clients can still work well. So our model can show high robustness.

(3) Mobile clients can feasibly choose storage servers and recover server according to the load of the storage servers and the state of network. So our model has good performance for load balancing.

(4) Our mobile database model can fulfill the mechanism of the least privilege. Both mobile clients and storage servers can hold the least privilege which greatly reduces the risk of data disclosure.

V. Experiment Results and Analysis

To perform simulation experiments we build an experiment panel. The CPU is Intel i3-413@3.4 GHZ. The memory is 4GB. The development environment is Eclipse Juno. The database management software is MySQL 5.6.

In experiments k and n of Shamir threshold secret sharing protocol all range from 0 to 20. The length of the key in AES algorithm is 128-bit. The number of mobile clients ranges from 10 to 100.

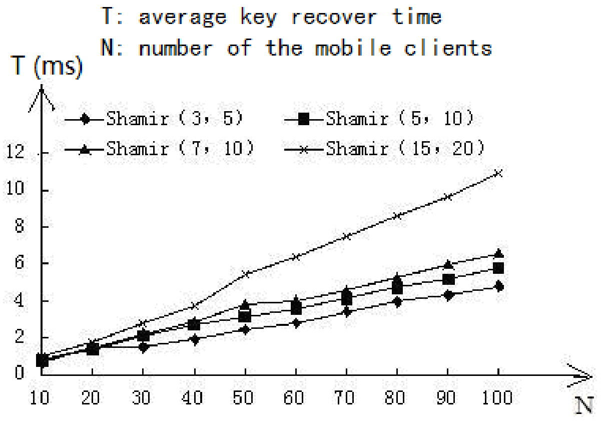

Figure 2. average key recover time----number of the mobile clients

. In Fig .2 the horizontal axis is the number of the mobile clients and the vertical axis is the average key recover time for the recover server to recover the key over 100 times. There are four curves in Fig .2 which represent the experiment results when in Shamir threshold secret sharing protocol (k, n) is (3,5), (5,10), (7,10) and (15, 20) respectively. It's easy to find that the average key recover time increases with the value of (k, n) increasing when the number of the mobile clients is fixed. On the other hand the average key recover time increases with number of the mobile clients increasing when the value of (k, n) is fixed.

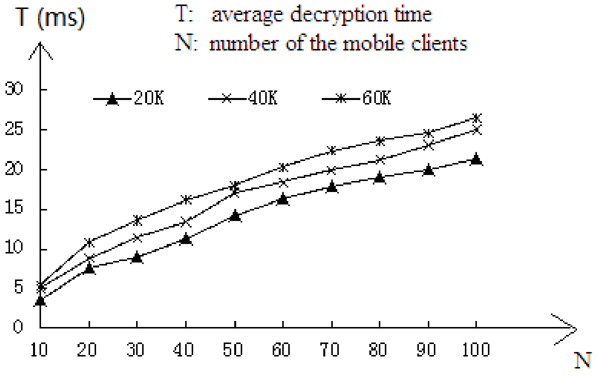

Figure 3. average decryption time—number of the mobile clients

In Fig .3 the horizontal axis is the number of the mobile clients and the vertical axis is the average decryption time for the recover server to decrypt the database over 500 times. There are three curves in Fig .3 which represent the experiment results when the size of the database is 20K, 40K and 60K. It's easy to find that the average decryption time increases with the size of the database increasing when the number of the mobile clients is fixed. On the other hand the decryption time increases with number of the mobile clients increasing when the size of the database is fixed.

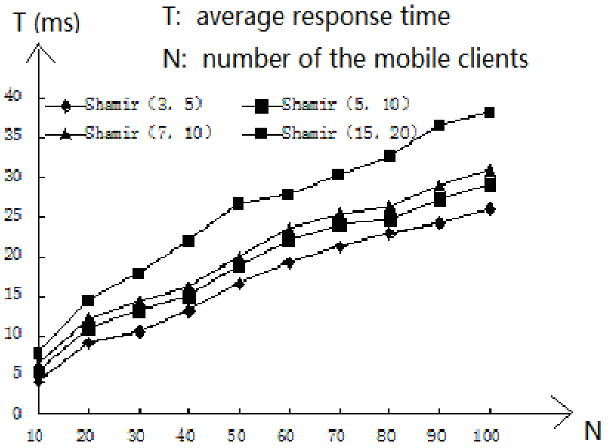

Figure 4. average response time—number of the mobile clients

In Fig .4 the horizontal axis is the number of the mobile clients and the vertical axis is the average response time for the mobile client to finish a data access over 500 times. There are four curves in Fig .4 which represent the experiment results when in Shamir threshold secret sharing protocol (k, n) is (3,5), (5,10), (7,10) and (15, 20) respectively and the size of database is 20K. It's easy to find that the average response time increases with increasing with the value of (k, n) when the number of the mobile clients and the size of the database are fixed. On the other hand the response time increases with number of the mobile clients increasing when the size of the database and the value of (k, n) are also fixed.

A very important fact is that the average response time linearly increases with the number of the mobile clients increasing. No exponential growth appears. So our mobile database model shows a good stability so that it can work well even if there are many mobile clients.

VI. Discussion and Cconclusion

In this mobile database model, people must create n copy of the database and store them on n storage servers respectively. So the memory consumption is inevitably large than the traditional mobile model, which is the necessary expense to gain a higher security and a higher robustness. On the other hand we can design a variant of the mobile database model which can overcome this difficulty. We can perform secret protocol not on the key to database but on the database itself. So the database is divided into n data blocks according to Shamir (k, n) threshold secret sharing protocol. The n data blocks are distributed to n storage servers. It's easy to notice that any data block is meaningless. For an attacker, to invade a storage server and get its block is not enough. He or she can't get even one piece of the data. The size of the sum of the n data block may be larger than the size of the database. But it's much smaller than the size of the sum of n database copies. The variant model needs lower memory consumption. But it faces another difficulty. When k storage servers have been chosen out, the n data blocks must be transmitted to the recover server. Obviously it means a large number of data being transmitted in the mobile network. As known the capacity of the wireless channel in the mobile network is usually limited. It can't meet such demands. So our original mobile database is easier to carry out in practice.

In this paper we present a mobile data model based on secret sharing protocol. By encrypting the database with AES algorithm and sharing the key with Shamir (k, n) threshold secret sharing protocol, people can disperse the database on n storage servers. When a mobile client wants to access the database, it must gets at least k storage servers' permissions, in which the k storage servers can be chosen out from the n storage servers at random. If an illegal user wants to access the database, it must invade at least k storage servers, which is very difficult. So our model can gain a high security against possible attackers. If a few storage servers collapse, mobile client can still access the database smoothly. So our model has a high robustness. The experiment results show that our model is feasible and it can achieve good performances with the number of the mobile clients increasing.

Acknowledgment

This work is supported by Natural Science Foundation of China (Grants 61472412) and Natural Science Foundation of the Education Department of Henan Province of China (Grants 14A520012).

References

[1] P. Gupta, P. Saxena, A. K. Ramani et al., "Optimized use of battery power in wireless Ad hoc networks", Phoenix Park, Korea : ICACT'10 Proceedings of the 12th international conference on Advanced communication technology. vol. 2, Feb. 2010, pp.1093 - 1097

[2] QIAN Xizhi, CHEN Zhibo, "Research on mobile database key technologies and application", Microcomputer Information2010, vol. 10, no. 2, Feb. 2010, pp. 89-90.

[3] Shan Wang, Zhiming Ding, Xiao He, "Mobile database and its application", Computer Application, vol. 20, no. 9, Sep. 2000, pp. 1-8.

[4] Jindong Wang, “Design and implementment of database encryption system based on advanced data encrytion standard AES”, Xian: Xidian University Thesis, may. 2011. pp. 21-30.

[5] A. Shamir, “How to Share a Secret”, Communications of the ACM., vol. 22, no. 11, Nov. 1979, pp. 612-613.

[6] Liang Zeng, “Research on verifiable secret sharing scheme”, Chang Sha: Changsha University of Science&Technology Thesis, Mar. 2011, pp. 27-31.

[7] Suyun Li, Runhua Shi, “A dynamic secret key sharing scheme”, Journal of Anhui University (Natural Science Edition), vol. 34, no. 3, Mar. 2000, pp. 38-42.

[8] Zhenyu Zhou, Shaojun Liu, Ziyan Wang, Xiaoqing Tan, “Implement of a threshold encryption scheme”, Modern Computer. Vol. 11, Nov. 2009, pp. 41-44.

[9] Yingying Mao, “Research on hierarcllical threshold secret sharing system”, Xian: Xidian University Thesis, May. 2009, pp. 2-6.

[10] Yun Quan, Miao He, “Application and implementation of servers load balance”, Micromputer Applications, vol. 27, no. 4, Apr. 2006, pp. 433-435.