Winter 12-1-2010

The Efficiency ,Technology and the Independence Study of the Database outsourcing Security Service

Yinxu Li

Huizhang Shen

Wayne W. Huang

Jidi Zhao

THE EFFICIENCY, TECHNOLOGY AND THE INDEPENDENCE STUDY OF THE DATABASE OUTSOURCING SECURITY SERVICE

Yinxu Li1 Huizhang Shen1 Wayne W. Huang2 Jidi Zhao1

1 Antai College of Economics & Management, Shanghai Jiao Tong University, Shanghai, China Email: rocky8641@hotmail.com
2 Department of MIS, College of Business, Ohio University, Ohio, USA

Abstract

Clients who adopt data outsourcing services tend to store their data in the media provided by the services providers. While through data analysis, author found that there're no reliable promises in data securities as the services providers could not assure that the outsourced information won't be disclosed by some third parties. Such as natural disasters 、some emergencies or crimes committed by in-house staffs and so on. Which means that if the information is stored in clear text, the risk of that the data might be disclosed or interpolated will always exists. Therefore, author point out that only when data stored in the cipher text form and the process of encryption/ decryption is managed by the users could guarantee the data real security and privacy. So it comes to the study of "efficiency, technology and the independence" in database outsourcing services when the users have to encryption and decryption by themselves. Based on the research and analysis of the problem, this paper tries to driving the solution of implementation strategy and methods.

Keywords: data outsourcing services、 information security 、efficiency、technology、provocateur

1 Introduction

Being an important component of the outsourcing services in the IT fields, information systems outsourcing services begin to attract wide attention from business community and academic area. In the business world, entrepreneurs are usually concerned about the benefits and risks of an information systems outsourcing、comparison between gains and losses and then make some decisions. In the academic community, scholars concerned about various management issues carried by the outsourcing, including the risk Management, implementation management and so on. For example, study outsourcing risk as a whole， like how to reduce the risk caused by the uncertainty in the information innovation and changing process; the risk of failure caused by the uncertainty business environment and the risk caused by improper HR management during the Business Process Reengineering. [1] [2]

There're also some scholars engaged in empirical research. For example, which variables affect the outsourcing companies' decision-making levels, What variables affect the process of outsourcing performance issues? [3] [4] [5]. However, most of the existing research just discussed how to increase the overall performance of information systems outsourcing and the success rate. While the problem of how to ensure the information security in the information system during and after the process of outsourcing is rarely being concerned. In this paper, author collect, analysis the security status of database outsourcing service, studied how to ensure the information security after the clients trustee the software and hardware to the services suppliers.

Under the data storage service provider's help, the clients can store data in the provided space and

completion the data processing tasks such as query, modify, backup and so on. Through this way, outsourcers can reduce the cost in technology investment 、 operation and maintenance costs. However, can the service provider ensure that the information will not be disclosed or be obtained by other parties? If there exists the risk that the service providers may tamper or leak data, what will be the future of database or even information system outsourcing.

On the clients side, the safest way in dealing with data is to gain the rights and technology of encryption and decryption while make it independent of the other parties. Can it be true? It means low efficiency when encrypting and decrypting data independently, can clients endure it? Also, outsourcing helps the company not to be involved in the technical aspects, does every company has the technology capabilities to finishing encryption and decryption process without outsourcing? Finally, can company be independent of the third party when developing and implementing the encryption and decryption tools? The three mentioned is the “efficiency, technology and the independence “problem that discussed this paper. Only after solving it can we fundamentally solve the outsource data security problem and ensure the sustainable development of the database outsourcing or even information systems outsourcing.

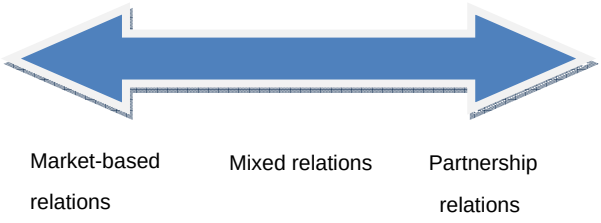
2 The classification of outsourced database

In 2002, Hakan Hacigumus and his colleges who came from the University of California (Irvine campus) firstly put the conception that “make the database as a service” [6], that’s out sourced database. And then, based on the internet, they built a prototype system called “NetDB2”. In this system, organizations run their database operations on the outsourced database server. The outsourced services providers offer the remote database services to the database owner and users including database creating、storage、update and query service.

On the user’s side, a outsourced database is equal to a common database management systems in the application layer while the data may be stored locally or be in one or maniple database servers through the network.

As a result, the outsourcing database system should also have the functions as data manipulation, data security protection, data integrity checks, concurrency control and so on.

There are many companies who provide the database outsourcing services now, including My SQL Hosting (Adhost.com), Microsoft SQL Hosting (discountasp.net), IBM Data Center Outsourcing Services (www-1.ibm.com / services), Web Database Hosting (open db. com) and so on. According to feature of assets specification and uncertainty, Robert kerlaypa and Wendell Jones defined the three-partnership model as market-based relationship、partnership relationship and the midway relationship in the "outsourcing the information systems, technology and services" [7] [8]. In this book, they regarded the relationship between the clients and service providers as a continuum.



Fingure1 the relationship between the clients and the service provider (1)

As shown in the figure 1, one end of which is "market-based relations". In this case, companies can freely choose the service providers who are able to finish to task. As the "market-based relations" usually has a relatively short period of the contract, that after finishing the contract, the company can turn to another services provider who has a lower cost or better services. On the other side is a long-term partnership relationship. In such relationship, a company and the service provider contracted repeatedly and established a long-term mutually beneficial partnership. Between the two cases is the midway relationship, it is necessary to hold or

maintain the long-term cooperation relationship until the completion of the primary tasks. Based the three relationships, there're three database outsourcing models.

2.1 Market-based relations

It usually present as a company makes a contract with a service provider to build a particular data center to fulfill its needs. In this case, enterprises and suppliers are usually experiencing a short-term co-operation process. The completed data center (information systems) and all the data will be stored and managed by the company itself. Most companies choose this form of cooperation in the early-stage of the development of information technology.

For example, the first case of outsourcing was that Kodak solved its information technology problem through outsourcing in 1994 [9]. At that time, some big companies including Kodak ask the IBM not only sold out the mainframe sales and the PC, but also help them to manage the entire IT system. Kodak, for example, put forward its own data center and technology center would be outsourced. IBM realized in time that it will be a potential chance, so the company called ISSC (Integrated Systems Solutions) was born.

With the development of the technology, the ISSC has now grown to an indispensable part of IBM Global Services (IBM Global Services). Making a simply request on www.Baidu.com, you can find thousands of outsourcing service providers such as ACCESS, SQL databases and so on. As desktop database like ACCESS has the superior in its object-oriented, easy to develop, user friendly and so on that enterprises can purchase and use the database management software and information systems at a cost-efficient price..

Now, many small businesses are willing to buy desktop database containing information systems, and maintain a simple and market relations with suppliers.

2.2 partnership relation

Another common form of data outsourcing type is partnership relation. Outsourcer (data owner) outsourced the services to the service providers ("server and administrator" in the fig2) including database, information processing, system maintenance and so on. System users (Owner and may include Customer of the owner) send data manipulation request from client to the service provider's server and then server return the result that the user needed. All the technology like system maintenance is provided by the employers in the service provider's side. This kind of data outsourcing type is usually called the third-party outsourcing. According to the characteristics, the third-party outsourcing belongs to the partnership relationship.

Usually, a typical partnership database outsourcing service is used in day-to-day application. For example, JDSU, a company well-known for its high-tech optical devices, signed an outsourcing agreement with Oracle's ERP in 2001, using the next IT cooperation mode of application service provider (ASP). In the process, Oracle's ERP took over the data management process and ERP software maintenance task of JDSU. As a result, JDSU decrease one-third of its IT staff. Also, this contract helps the company eliminate the investment in hardware, minimizing the damage from updating and make the company focusing on the services.

Till now, Oracle can almost handle every day-to-day operation within the contract, including financial data, human resources and so on. Though the server is far in the United States of Tennessee, Austin [11], JDSU staff can enter into the Oracle database and ERP software via the internet all over the world.

2.3 Mixed relations

Mixed relationship is the type that between the market-based relationship and partnership relationship. It has a variety of concrete forms.

One common form of it is that after outsourcing the data, users by their selves retain and store the data and collect the additional information as well.

While concerning the operation needs and the security when facing with the emergency, service providers will back up the data and the transaction. [12]

3 security issues of data outsourcing

3.1 Data Security and the survival of the enterprise

Data and information play an important role in the survival of the enterprise, sometimes they are even more important than HR and should be given due attention and protection. According to the IDC statistics, 55% of the companies which faced with disaster and lost data in the past 10 years in United States bankrupted at time, The remaining 45%, due to data loss, 29% also closed down in less than two years, There're only 16% can survive. the international organization Gartner Group survey also shows that companies experienced large-scale data losing disaster will usually cause the company fail to continue the operation. 2 / 5 of them were never resumed operations, while 1 / 3 of the remaining companies were also end in bankruptcy in two years [13] [14].

On September 11, 2001, the World Trade Center Twin Towers suffered the fight against terror that no one can predict. Before the suddenly disaster and destruction, there were about 350 enterprises working of the World Trade Center. One year after the disaster, there were only 150 enterprises continue working while the other 200 companies disclosed and disappeared because of losing the critical data and the destroyed the important information system.[15]

3.2 The forms of database attack and the existing preventive measures

Take the partnership relationship of outsourcing as an example, there might be four attack forms.

Attacker A could theft the password form legitimate users and then enter the client side to steal of tamper information. Attacker B could theft the information administrator's password from the services providers so as to pretend to be a legal administrator then do harm to the database. Attacker C usually intercepted the database information from the communication channel between the client and the server. Attacker D may aim at the physical database and bypass the server management system.

Now, the most common database security protection measure is to restrict access to the database or limit the authority such as access control and so on.

We can find out that the client can identify the right user to prevent an Attacker A, on the Server side, server can validate whether it is legitimate or not and then prevent an attacker B.

Access control means with the combination of hardware and software technology, restrict the database users or user's authority in order to ensure the data security. A typical access control software product is a firewall while the typical access control hardware (or a combination of hardware and software) products is the IC card. It is used to store the user's personal private key, effectively identity of the user. At same time, it can also realize the personal digital signature mechanism based on the combination of the private key and digital signature technology.

With the development of pattern recognition technology, many high-technology identifications such as fingerprints, retina and facial features will be put to use. If combining such high-technology with the existing measures like digital signature, it is bound to improve the users identification and validation mechanism then finally achieve the aim of access control and protecting the data security.

The measure mentioned above is limited as it could only prevent the attacker A and the attacker B. as attacker C and attacker D bypass the preventive measure and attack the operating system level and the access to the database documents. Some extremist examples might be that they thieved the hard drive or the data storage part. The common effective way to prevent the attacker C and D is using

the digital encryption technology based on cryptography. Even if the attacker stolen the data files, as the data is stored in the form of dense text, attacker can't directly get the information.

In the field of military and national defense, encryption is common adopted during the data transmission to prevent the attacker C while top-secret data files in some departments and enterprises in also being encrypted before storing to prevent attack D.

3.3 The information risk after outsourcing to a third-party

On November 14, 2006, Ernst & Young released a survey called "global information security" on 1,200 public and private institutions form 48 countries, showing that most business failed to manage risks from the third party though they began to release the necessity to invest on data protection and information security. [16] [17] when the institution had added the problem of keeping data security in the top important list, there is no uniform conclusion on it.

There are not just hearsay, but are likely to taken place in a person you known.[16] According to IT security experts that hackers have become more sophisticated and globalization, some crime organizations might even employ hackers from Eastern Europe and South America to theft the identity and credit card information. [18]

For example, researchers from the UK at Cardiff University (Cardiff University) found that the Hong Kong Bank (HSBC) online banking system had the blemish they call "loopholes" that private detectives were able to buy the customer records from India call center.

The Ernst & Young study also found that although many organizations are beginning to understand that it is necessary to invest on IT security, most of them still take no action on third-party risk management. About 55% of the companies acknowledged that they didn't make any formal agreement with the third-party suppliers.

The survey also found that the largest hidden troubles of information security existing in the field of new technologies like removable Memory media such as mobile computing, wireless networks and so on.

As a result, though people has recognized the importance of information security assurances, it is an unavoidable topic to protect the information security from new technology and other threats and it will also be the next study focus for the information services providers. [16]

3.4 Encrypted the physical database of the third-party and its problems

According to the analysis of 3.2, based on the aspects of data privacy; the safest way is to encrypt the physical database. There are several encryption methods of it and this paper lists the widely used styles as follows [19]:

A Encryption on the service provider's side

The service provider is responsible for data encryption, when a hacker attack, and even stole the hard disk, even if their access to the encrypted data that can not crack the cipher text through brute force attack a short period of time. However, in this mode, the database outsourcer can not master the database encryption; it is entirely arranged by the service provider.

Although the services provided to promise that the outsourcing of information will not be disclosed to people from other parties, a thief within a house is hard to guard against.

B Encryption on the outsourcing side

The clients can choose to encrypt the database themselves, while storing the encrypted data in the physical medium provided by the services providers.

Its advantage lies in that data is encrypted that not only hackers but also the service provider can't access to the real text while the decryption key is managed and maintained by the outsourcing side. In order to get the information, the attackers needs to gain dual key—the decryption methods and the authority to access which increase the difficulty of illegal access and ensure the data security.

According to the FBI/CSI2006-year survey of information security, [20] there are currently 48% of the database users have the option to encrypt the database themselves. There are approximately 31% of them choose some end-use encryption software to encrypt data. This kind of data-encryption can be regarded as the encryption on the outsourcing side.

C Encryption at both ends

Encryption at both ends is a combination of both methods mentioned above. The advantage is that the double encryption process has greatly increased the difficulty to break the data. While compare to is advantage, it can be figured out that both-ends-encryption does not always represent the "1 +1> = 2"effect. In fact, this process will increase the maintenance /management costs in actual use and leads to the lower efficiency in the client's side.

Based on the above analysis, when talking to outsourcing side, it is more safe and assured for them to encrypt by themselves. However, there're some problems in the style. The three major difficulties are that:

Firstly, in addition to more processing time in the client side, such type means the increasing cost and reducing the efficiency.

Secondly, the services providers must acquire a certain amount of outsourcing of information security knowledge, the ability to choose suitable encryption strength, the encryption scheme and encryption algorithm. It means the possibility of leakage if providers recourse encryption process to others,

Thirdly, the data encryption software is often not independent of the service provider side or even developed by the service providers. This likes to buy a suit of key and lock from one locksmith and we don't know whether there are spare keys in the locksmith's hands. Is it secure?

The three difficulties can be summed up as: "the efficiency (against the database outsourcers), technology (against the database outsourcers) and the independence (the database's encryption process outsourcing can not rely on the service provider)," Only after solving the three difficulties can we promote the mode of encryption on the database outsourcing side and fundamentally solve the problem of database outsourcing security. This paper will study the possible solutions later on.

4 Traitor thieves

If the commitments from the service provider's side that they promise no leakage of the information from the outsourcing side to other parties is true, there three difficulties mentioned above is not existed. However, the truth is always different; the problem doesn't lies in the lack of credit but in the existing of traitor thieves that service providers can't ensure the 100% security. Here are some evidences:

"Yahoo! BB" is a network service created by the Japan Softbank and Yahoo Japan. According to the local newspaper on December 26, 2006, "Yahoo! BB" has become a huge extortion victim. The Softbank recognized that more than 4,500,000 person's information was leaked including Yahoo! BB current and former users. The police had arrested 4 suspects in connection with the case, all of them were the employees of the database services provider— YAHOO. [21]

"IT Times" had reported that Taiwan Semiconductor Manufacturing Company engineers have taken place in an attempt to steal confidential corporate data. [23] As the enterprise installed the CA enterprise management software, the engineer did a futile effort and ultimately failed.

CCTV "3 • 15" party expose the source of the spam messages on March 15, 2008. According to the report, one company called Focus Media Wireless Technologies, Inc. (a subsidiary of Focus Media) said that "There is a Club in the Beijing where company brought the information including the name of the deputy General Manager, directors, the place and floor of their house and so on. [24]

In addition to the traitor thieves, the oversight from a third-party database service provider in the day-to-day management is also a big problem that can not be ignored.

Considering the cost, database outsourcers take over its data storage to the third party. With the

development of IT, the cubage of data storage hardware with a large amount of volumes is constantly decreasing; the losing of such hardware or related products will cause a huge problem and crisis to the business. Such cases are countless. Take the banking industry as an example:

On February 28, 2005, United States banks (Bank of America) claims that they lost the backup computer tape included about 1,200,000 federal employees' personal data. [25]A spokesman of the bank said that computer tape was lost when move to the back-up warehouse in December last year.

The New York Times edition of Science and Technology reported that spokesman of the United States of bank said the bank does not believe that such information will be stolen or fall into the hands of the criminal fraud. At present, the affected bank accounts have no suspicious behavior. In addition, on June 6, 2005, the United States, Citigroup disclosed that the group lost a record including 3,900,000 customers' accounts and personal information. [22] [26] prior to less than a week, on June 1, 2005, the Swiss banking group lost a disk in its Japan including" highly sensitive" customer information. [27] These events are a wake-up call for us, if the enterprise uses third-party database management in the form of outsourcing, not only in the need to guarantee the security of software systems, but also must be stored in the database of third-party content into measures such as encryption, Thereby reducing the risk of information leakage when the storage medium is lost.

5 The features of database outsourcing services "efficiency, technology and independence"

Considering the problem of traitor thieves, outsourcers' need a special kind of database encryption method, the "special" in its performance means it should solve the "efficiency, technology and independence" problem. Here is an example to illustrate its characteristics using non-professional terms.

Assuming a customer to rent a strongbox from the bank, the bank promises: Only the user can open the strongbox, bank staff can not open the it, so only customers themselves know what they store and are able to put in/out.

How to let customers believe it? Bank staff to allow users to check:

A one (six-plane) strongbox has only one door, the other five plane are closed to the surface (there is no way to see what's inside the door from the outside, strongbox is strong enough not to be broke);

B, there is a safe locks, the password is set by user selves;

C user brings his own padlock and lock outside the strongbox

As a result, even though things are stored in a bank strongbox, but it is managed by users' own. Bank staffs are not only having no access to the customers' items, but also customers can not see what is stored.

it is efficiency because though there're two locks, but it doesn't increase the manage trouble compared with other strongbox so that the users can accept.

When talking about the "techniques", it is easy to implement the process of setting up a password together with a lock. Considering the "independence", even if the bank's staff set a back door on the strongbox (For example, in addition to its own password, staff can set another one), as the customers brought about another padlock and the bank's staff certainly not the key, so it ensure the security.

Depicting their characteristics with terms:

1. The database encryption time is less or equal to the current common data encryption run-time; anti-strike capability (the security) is greater or equal to the current common encryption standard. The two different are the "efficiency."

2. To the database outsourcers, the way to access to the database through the outsourced database need to be the same as the traditional visit to the local server. So users do not have to change habits and the existing system as well. The encryption will not intervene in the operation of cryptography and is no additional burden on the technology. For service

providers, the encryption and decryption process are completely implemented by the database outsourcers that server only need to tackle with cipher text operation, so its applications are just the same as the original measure without encryption. In other words, though adding the encryption and decryption process in the clients' side, there're on influence on the server. For example, the clients query a result the server-side using cipher text and the server just need to deal with the cipher text. This is the "technology."

3.As the client has not changed the original system, the server side also

not changed the original applications, so the client encryption part can be regarded as a part of process independent of the client-side and the server-side. It can be provided by "other side" instead of the outsourcing service providers, which indicates "independent".

On data operating level, Hakan Hacigumus and other people put up the idea of "the database as a service", they brought forward a step-by-step outsourcing query strategy under the database outsourcing mode. [28] It has a relatively high feasibility and safety while its limitation lies in that it has to find the balance between the security and efficiency. On data concurrent control level, Li Xiong and other scholars studied the concurrent control problem for the outsourced database in the multi-client and multi-server network model [29]. In that paper, author put forward standards to measure the model of outsourced database with multi-client and multi-server. Including the accuracy, effectiveness and safety and at the same time put forward the concurrent operating mechanisms and the agreements to realize the inter-library aggregating operations (like max, min, selection of top k and so on)in a number of private databases. Then they computed and analyzed the accuracy, effectiveness and safety, through their experimental model.

In data security level, being the key problem of database outsourcing, there're many research on it. Because the database administrator from the service provider side has the full rights of the operations, the client have to validate the correctness and authenticity of the data. Giuseppe Ateniese, Randal Burns, and other researchers studied the problem of verify the authenticity of data return by a suspect server and put forward a verification strategy about data format independent PDP (Provable data possession). [30][31]

However, the research problem of the outsourced database security, in "efficiency, technology and independent" is still a new subject.

6 the solution of the "efficiency, technology and independence" problem

This article describes an algorithm to solve the "efficiency, technology and independence," problem by adding a plug-in software. It is called the rack and pinion encryption algorithm [32]

As shown in Figure 2, adding a plug-in will can help to encrypt and decrypt the outsourced database system, take the rack and pinion encryption algorithm for example, it will be used as a stand-alone plug-in.

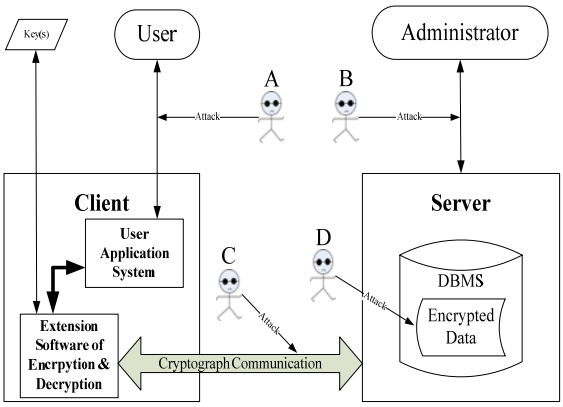


Figure 2 Adding a plug-in in the outsourced database system for encryption and decryption

After embedded it in the original, no-encrypted database system, it will first check the attributions of the database that is get the relevant information about the plaintext. According to the parameters of the plaintext, asking the client to set the number of the

pinion they need to encrypt. Based on the information tips, it is a simply request. Then the user still follows the clue to choose the different algorithm for each tooth of the pinion and set a password for the tooth as well. To the users (the database outsourcers), they have finished the encryption tasks. In order finish such task, clients don't have to take some specialized training. So the problem of technology in "efficiency, technology and independence" has been solved.

Considering the system security, the information (keys) set by the clients: the numbers of tooth of the pinion, corresponding algorithms and the secret (password and key) will neither store in storage device of the server nor in the client side. They will be stored in the user's moveable storage medium such as flash memory. Whenever the users need to operate the database, then they plug in the keys. To attack A, though he access to the system, he can't get the information of the database without the keys. To attack B or traitor thief, they can just get cipher text instead of plaintext. To attack C and attack D, they can only take the cipher text at most. To the database outsourcer, the combination of the different teeth, the encryption algorithm and the secret keys can not only reduce the risk of the data breaking but also avoiding the problems of traitor thieves in the service providers' sides. That increases the database security and privacy.

In paper "A Pinion-rack Encryption/Decryption Model for Database Security", it had already discussed the problem of "efficiency". The time cost for encrypting is equal or less than the current data encryption time. The anti-strike capability (the security) is greater or equal to the current common encryption standard. Using the model can reach the same security to the traditional encryption model with a relatively shorter secret key length. Moreover, the time to process a circular program is usually longer than the time needed to process an equivalent sequential program because CPU has to spend some additional time to judge the cyclic times, set and save program breakpoints. To the services providers, each encryption algorithm on the fields is simply and can be complete in the clients' side while the cipher text will not increase the data. So the Pinion-rack Encryption/Decryption Model greatly reduce the management and operation cost which is also a kind of efficiency.

The encryption and decryption plug-in can be developed or provided by the third party besides the database services providers. As the third party doesn't not involve in the operations of the outsourced database, so it is "independent".

In addition, the developers themselves can't crack the plug-in based on the Pinion-rack Encryption/Decryption Model, so there is no "back door" in the software which eliminate the possibility that the developers cracks the database form the "back door".

Conclusion

To sum up, though there're commitments from the service provider's side that they promise no leakage of the information from the outsourcing side to other parties, but the commitments may not be reliable.

The problem lies in the existing of traitor thieves, some unexpected disasters or the losing of the physical storage devices that service providers can't ensure the 100% security. So the data are under the threats of data leakage or tampering which cause the unpromising future of the database outsourcing and information system outsourcing as well.

The only way to let the database outsourcer entirely convinced that the data they stored in the service providers' devices is absolutely safe is to truly hold the key of the strongbox in hands. The database outsourcing services including the encryption algorithm that can solve the "efficiency, technology and independence" problem and algorithm's implementation strategy is the guarantee of the survival and development of the database outsourcing and information system outsourcing.

All the encryption algorithms and their implementation strategy that can solve the "efficiency, technology and independence" problem can be used to solve the information security issues

for the database outsourcers. Pinion-rack Encryption/Decryption Model is one of them.

Reference

[1] Zhu Wei. The implementation of software process management in the outsourcing project. Tongji University postgraduate thesis 2006-1

[2] Li Zhaoying. Analysis software outsourcing issues based on economic theory[N] Operational economic and technology 2006-4

[3] Cui Qiliang, software outsourcing: from service providers to the partnership[N] Information industry 2005-7（P10-12）

[4] Huang Shujun, Analysis on Bank information outsourcing decision postgraduate thesis 2006-4

[5] Huo jianguo, <China's foreign trade and national competitive advantage >[M],China business press, 2004, version1

[6] Hacigumus H, Iyer B, Mehrotra S. Providing Database as a Service. In:Proc. Of ICDE, 2002.

[7] [America] Robert • Clepper, Wendell • Jones, Yang Bo, M.. Information technology, systems and services outsourcing [M]. Beijing: Electronics Industry Press, Beijing

[8] Xu Qing, software outsourcing process type analysis [OL] IT world 2007-6

[9] Wang Xiangyong, consultant's value adding - in IBM's Life [N / OL] Computer World Net 2007-9http://www.ccw.com.cn/htm/work/corporation/01_9_25_2.asp

[10] Xie Min, database outsourcing, a new opportunities and challenges [J / OL] 2007-12

[11] Wu Ying Heng, ERP benefits of outsourcing to JDSU [J / OL] optical News http://www.ofweek.com/News/ 2006-08 / 20060830100257191.html

[12] Zhao Xin, Introduction of disaster backup database[N / OL] http://www.ofweek.com/ News / 2007-09/200709348457678.htm 2007-9

[13] IBM Support guide http://www-900.ibm.com/cn/support/guide /whitebooks

[14] Gartner Co,ltd， Analysis on China outsourcing market [P/OL] 2006

[15] Mo yunfei, importance of the data backup, China security information, http://bbs.hacker.cn/thread-29833-1-1.htm

[16] Ernst & Young, "Global Information Security" [P / OL] 2007-1

[17] LIU Yan, the survey showed behind awareness of global corporate IT security [N / OL] Sina Technology 2006-11-15,http://tech.sina.com.cn/ it/2006-11-15/07471237453.shtml

[18] Wu Yue, Information Security overview [N / OL] SAN 2007-2-16 http://tech.sina.com.cn / Info/Securty/2006-11-20/1163989319d38835.shtml

[19] Zhang Feng, hold your secret data - storage encryption technology overview [N / OL] Network World http://www.cnw.com.cn / cnw07 / Server Storage

[20] FBI/CSI 2006 Security technologies used http://www.i170.com/Article/34116

[21] Pacific technology news groups, Softbank earthquake: more than 400 million user information seriously compromised [N / OL] 2006-12-26 http:// www.pconline. Com.cn / news/nw/0403/324419 . html

[22] Min Zhou, MasterCard information leaks [N / OL] 2005.06.23 Beijing Information Report

[23] Hu Yaqing, how to prevent internal data leakage by applying IT Management 2007-7-26 http:// www.chinalabs.com/view/ZXKM0RPO.html

[24] CCTV.com, Focus Media made hundreds of millions of spam messages a day [N / OL] Quanzhou Evening News March 19, 2008

[25] Ccident net. http://market.ccidnet.com/ market /article/content/406/200502/113219.html 2005-02-28 10:24:13.0

[26] Ccident net http://tech.ccidnet.com/ 2005.02.28

[27] China Net http://www.china.com.cn/chinese /FI-c/876984.htm 2005-5-31

[28] Hacigumus H, Iyer B, Mehrotra S. Executing SQL over Encrypted Data in the Database Service Provider Model[C]. The ACM SIGMOD International Conference on Management of Data. Madison, Wisconsin, 2002:216-227.

[29] Li Xiong, Subramanyam Chitti, Ling Liu. Preserving Data Privacy in Outsourcing Data Aggregation Services. ACM Transactions on Internet Technology, Vol. 7, No. 3, Article 17, Publication date: August 2007.

[30] Giuseppe Ateniese,Secure and Efficient Group Communication in Wide and Local Area Networks:[dissertation].Italy:Univ.of di Genova,1999.

[31]]Randal C Burns, Robert M Rees. Safe Caching in a Distributed File System for Network Attached Storage[A].

[32] Huizhang Shen, Jidi Zhao, Wayne W. Huang, A Pinion-rack Encryption/Decryption Model for Database Security, Journal of Database Management, 2008