Database Security System for Information Protection in Network Environment

Myung-Jin Jung[a], Chung-Yung Lee[b], Sang-Hyun Bae[c]

[a]Dept of Computer Science & Statistics, Chosun University, Gwangju, 375, Korea
Tel : +82-062-230-7962 Fax : +82-062-234-4326
E-mail: cssnever@empal.com, lk518@hanmail.net, shbae@chosun.ac.kr

Abstract: *Network security should be first considered in a distributed computing environment with frequent information interchange through internet. Clear classification is needed for information users should protect and for information open outside. Basically proper encrypted database system should be constructed for information security, and security policy should be planned for each site. This paper describes access control, user authentication, and User Security and Encryption technology for the construction of database security system from network users. We propose model of network encrypted database security system for combining these elements through the analysis of operational and technological elements. Systematic combination of operational and technological elements with proposed model can construct encrypted database security system secured from unauthorized users in distributed computing environment*

Keyword: Data base security, Protection in Network Environment

1. INTRODUCTION

Computer development and internet expansion have advanced informational society, and have promoted the development of functional elements. Eavesdropping and forgery of information have prevented the development of informational society.

The concern of information protection has been raised up as the processing and interchange of information have been activated in network environment. Database security problem has occurred in distributed computing environment as information protection system environment has been extended complicated, and the construction of technological and institutional information protection system has been needed for the orientation of proper use and management of information.

Security can be largely classified into information protection based technology and system network protection technology. Information protection technology to solve the side effect of informational society is concerned with wide area including encryption algorithm, information protection system, public key based structure with the reliability of public key, virus and technology against hacking, digital watermark technology to protect knowledge property, and application technology for information protection of electronic implementation of existing paper currency into electronic currency. System network protection technology can be classified into security concerned with internet, Establishment and audit of security policy, system construction and encrypted database security according to it, and security consciousness of each user are basic elements for information protection in network. Next generation aggressive information security technology, intrusion prevention system, and intrusion detection system [1].

In this paper, we describe access control technique, user authentication technique, and user security technique for the protection of encrypted database from unauthorized users.

2. DATABASE SECURITY

Threat against information protection has increased with rapid development of internet and open network system, and thus the necessity of security has also increased. The countermeasure of information protection against the threat should be taken systematically for legal, institutional, administrative, and technological information protection[2][3]. Especially, access control, authentication and discrimination, intrusion detection technology, encryption and key management, and virus and hacking prevention should be emphasized for user information protection.

2.1 Authentication

User authentication is the process to confirm if a person registers actually. Individual or user authentication of communication network including internet is made through code use in log-on. A person knowing the code is considered as a reliable user. However, a weakness of authentication in electronic commerce is that code is stolen, known to others, or forgotten. User authentication has the premise that user ID and password is encoded and user is confirmed by the comparison of decrypted result of database with encrypted accounting. These kinds of authentication is generally maintained two kinds of elements in security. The methods are the ones by key and by IP. User authentication is the basic items regulating access control or user mandatory and is the first step for

defense.
User authentication process is the confirmation shared accounting between user and application or system program. Client and server needs authentication in distributed computing environment. User should get an authentication from server, when he requests a service from it. In cases, server also should get an authentication from user, which is call Two-Party authentication in which additional authentication server manages all the passwords that is called Third-Party Authentication[3].

2.2 Access control

Access means the authority with which user can access particular system object such as directory or file. ACL(Access Control List) is the list established to inform operating system of computer of this access. Each object has security property to discriminate access control list, which has an entry for each system user with access authority. General authority includes read, write, modify, delete, and execute one file or all the files in one directory. Each ACL has one or more access control entries consisting of user's name or user group. User can become names indicating the roles such as programmer or tester. Access control policy can be classified into arbitrary access control and compulsory access control depending that access authority are given by resource owner or system administrator[4]. Arbitrary access control policy is the mode restricting the access to subject or object based on it. That is, access control is made by object owner arbitrarily. Therefore, subject with any access authority can give its authority to arbitrary other subjects. Compulsory access control policy is the mode restricting access to the object based on formalized authority secret information included in object.
The decision criteria if system allows requested access or not is as follows:

Table 1. Access control decision criteri

Decision criteria		Contents
Account		System access is controlled through ID confirmation and authentication process
Service restriction		Restriction predefined by resource owner or administrator
Access Format	Subjects	Individual user, user group, host, terminal, application program
	Objects	Ones to be controlled for access include database, file, and program
	Access authority	Subject to access for read, write, delete, execute
Location		Access to particular resource of system is determined based on physi cal and logical location
Time		Access is restricted some day a week or particular period a day

2.3 User security

The weakest element of information security system components is human one. Internal threat is larger than external one in distributed computing system. Internal threat can be caused by user's error or carelessness, and equipment or information can be leaked externally illegally[4]. Therefore, internal user management can make an effect on system security.
People treat establishment, operation, and backup of system of regular job, plan, security policy, etc. Damage cases have been increased of information system by internal users, and their detection is very hard to find out. Especially, the damage by system administrator and programmer is hard to detect. The damage can be minimized by granting authority of data integrity of individual system and security regulation observation in user's database security for information protection system.

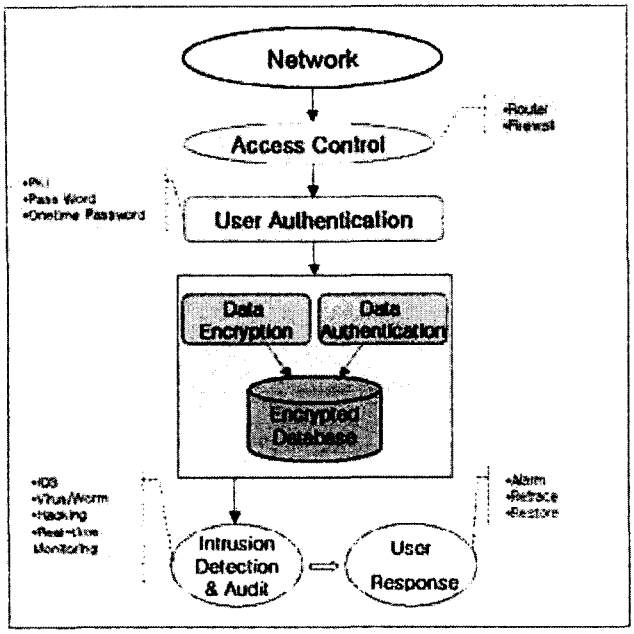
2.4 Encryption technology

Encryption plays an important role for data security in distributed computing system. Basic functions of encryption are authentication and information protection. Authentication is the function to confirm legal receive of message from legitimate sender without its illegal forgery, and information protection keeps data secret.
Encryption technology is one of core technologies for information protection, and is concerned with encryption algorithm largely providing data secrecy. It is largely divided into secret key code of DES(Data Encryption Standard) and public key code of RSA(Rivest Shamir Adleman). Secret key can be classified into block and stream codes, and public key into Knapsack problem, lattice, knot theory, etc[5][6].

3. PROPOSED SYSTEM MODEL FOR INFORMATION PROTECTION

While data share through network in distributed computing environment are common in real world, the risk of data integrity and security have increased in network environment. We propose encrypted database security system model, which secures data from unauthorized users in this network environment(Fig. 1).

Figure 1 encrypted database security system Model



3.1 User authentication and authority

User authentication is made by Kerberos 5 DCE provides in distributed computing environment, and authority confirmation is implemented using ACL function DEC provides. User information, password information, and ACL information can be stored in DCE Registry DB[7].
The process of user authentication and authority confirmation is as follows(Fig. 4).

·Security manager registers user in registry database using registry editor.

·Application manager makes name of individual or group for access control to object such as application, file, or directory using ACL editor.

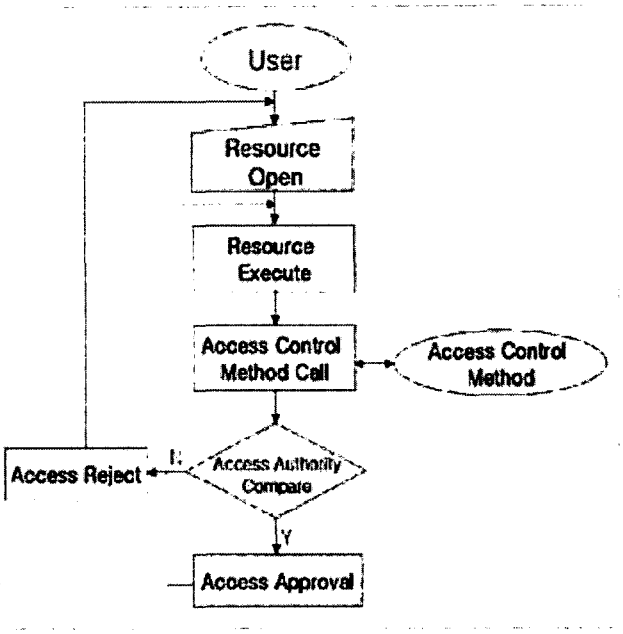
·When user logs in authentication server, Login process is connected to authentication and authority server through user confirmation to obtain ticket to access other server.

·Authentication server and authority makes authentication to access other server after user's authentication obtaining user's secret key and authority property from Registry Database.

· When user begins application client, user's ID and authority property are presented and authentication is received from server.

· Application server determined user's authority calling ACL manager.

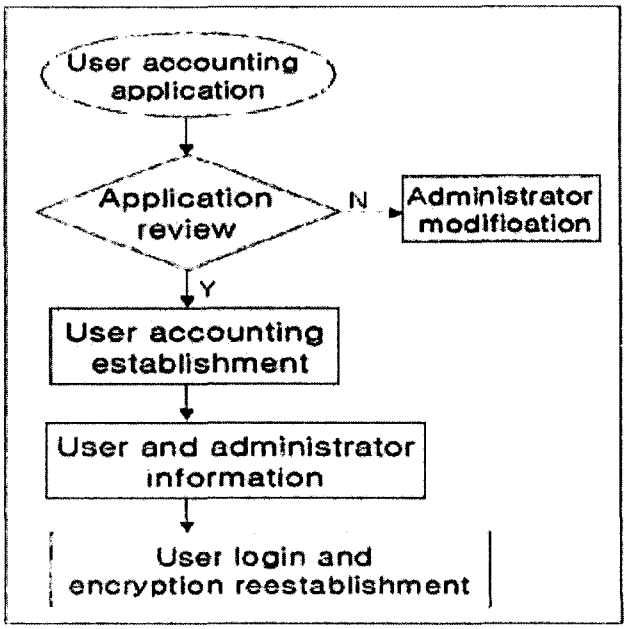
Figure 2 User authentication and authority



3.2 Database access control

In this paper, we present many access control techniques. Here, we describe access control of resources. User or application program requests resources open. File system performs open process. In open process, access control technique is called, and it compares and checks user's requested access with user's access authority. Here, ACL or other access control mode is used. Access is accepted with access authority and rejected without access authority and again requested open(Fig. 2).

Figure 3 User access control



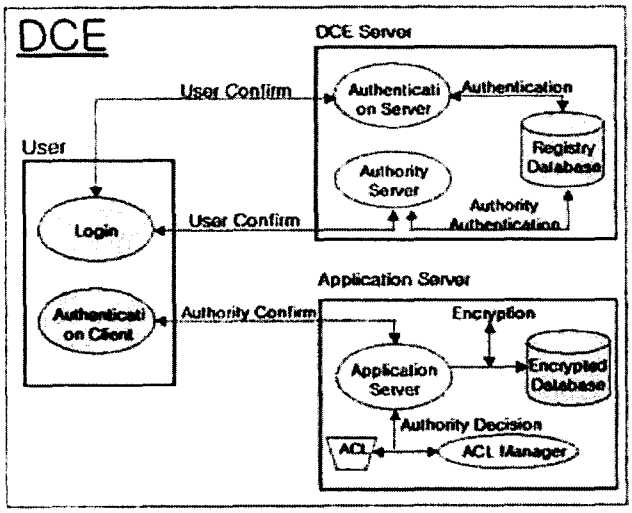
User should get accounting for information protection system in order to obtain user's access authority. The accounting should be established to give access authority

to concerned user. The process should be entailed to remove user's access authority. The process completes accounting generation after referring to grant and removal of user's access authority.

3.2.1 Database access authority

Figure 3 represented below is user's access authority process fir information protection system. Administrator of users presents accounting application to security manager. If security manager considers that the application is valid, he establishes accounting and informs concerned user of the fact. Next, user logs in and reestablishes encryption.

Figure 4. User access authorities



3.2.2 Database accounting establishment

Security manager requires accounting occurrence and management utility to establish user accounting. When concerned user inputs ID, manager brings about ID according to standard for information system operation environment. When user's access authority is inputted, security manager input name of group of user, which automatically produces user's access authority. Initial password is produced for accounting. When user logs in for the first time, his password is required to be reestablished and is expired in specific period. Any additional information input should terminate concerned utility.

3.2.3 Database accounting removal

The immediate user needs not to access information protection system any more, concerned user should inform security manager of it. Next, accounting generation and management utility are requested to remove accounting.

3.3 Database security

User security regulation proposed describes the regulation applied in developing user security policy for information protection in distributed computing environment. The regulation is consistent with user security policy. User security regulation is the subset of user access management needed for an implementation of user security policy. The regulation for information protection in a distributed computing environment is classified into user access, user account and management, and confidential management.

3.3.1 Database access regulation

User access regulation is as follows:

·User will be grouped based on job function. These groups is allowed only access required to perform concerned job.

·User is allowed only access to application level service.

·User is not allowed direct access to any service operating as a route.

·User is not allowed access without proper DCE Privilege Attribute Certificate.

·User does not have any authority the immediate his employment expires.

3.3.2 Database accounting management

User accounting management is as follows:

·User ID is drawn up according to standard algorithm. User ID does not include user name or number partially or wholly.

· Encryption for network authentication service requirement should include at least one digit and one special character in maximum length to be allowed by selected implementation.

·Encryption expires in specific period.

·Encryption should check the strength through cracking utility.

3.3.3 Confidential management

Confidential management regulation is as follows:

·If user logs out from information protection system and does not take any action during specific period, his ticket and PAC expire.

·DCE ticket and PAC is not allowed to exceed specific period.

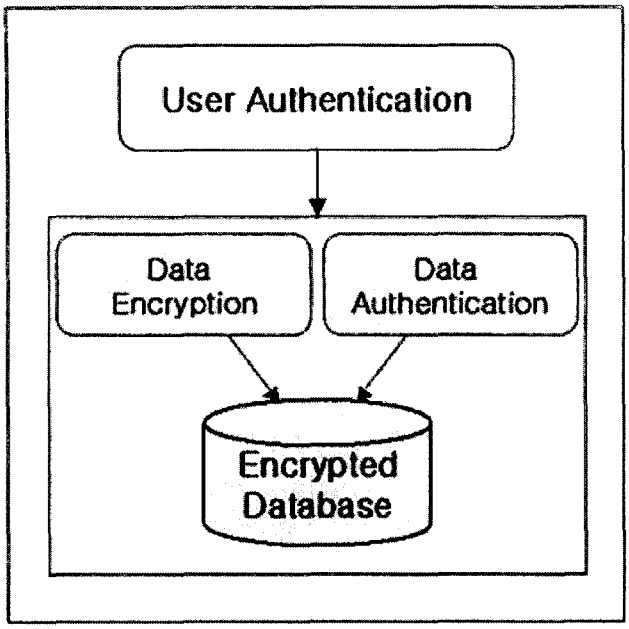
3.4 Encrypted database

Encryption plays an important role for network security in a distributed computing environment. Basic function of encryption is authentication and information protection. Authentication is the function to confirm legal receive of message from legitimate sender without its illegal forgery, and information protection keeps data secret.

Encryption technology is one of core technologies for information protection, and is concerned with encryption algorithm largely providing data secrecy. First of all, user is discriminated if he obtains valid authority to connect database or not. Valid user is given proper authority and performs encryption job connecting database. Using a given key for user to perform encryption job, they are stored in database after encrypted. On the reverse, user given a valid authority obtains original information connecting information stored in encrypted database(Fig.

5).

Figure 5. encrypted database



4. CONCLUSION

In this paper, we proposed model of encrypted database security system from network user. The following should be considered for the construction of encrypted database security system for information protection.

·Systematic and synthetic access mode is necessary.

Security is composed of various areas, and these components are combined organically to achieve aimed security level through mutual complement.

·The construction suitable for environment should be introduced.

When user access control is made for encrypted database security system, physical secure place as well as software method such as password should be considered.

·Whole cost should be reviewed enough.

The cost of development or product purchase cost policy should be estimated systematically in the construction of information protection system.

·User's consciousness for information protection should be recognized.

The recognition of information protection should have first priority, for which user's obligation and charge should be given through persistent user's instruction.

When the conditions to be considered are reviewed enough in the construction of database security system, we think that encrypted database security system can be constructed for information protection in a distributed computing environment.

References

[1] Hag-Bum Kim, System/Network Security: Access Control Technology, pp131-157, 2001

[2] Schneier, Bruce, Applied Cryptography: Protocols, Algorithms, and Source Code in C, pp417-454, 1995

[3] Stinson, Douglas R. "Cryptography : Theory and Practice", 1995

[4] AlfredJ. Menezes, PaulC. van Oorschot, ScottA. Vanstone "Handbook of Applied Cryptography", pp385-424, 1996

[5] NIST, "An Introduction to Computer Security : The NIST Handbook" ,pp183-246, 1999.

[6] R. Bird, et al.,"Systematic Design of Two party Authentication Protocols", Proc. of Crypto'91, pp.44-61, 1992

[7] Stalling, William, "Cryptography and Network Security 2/E H/C" , Prentice-Hall, 1998

[8] R.M.Davis,"The Data Encryption Standard in Perspective", Computer Security and Data Encryption Standard, National Bureau of Standards Special Publication, Feb 1978

[9] W.Diffie and M.E. Hellman,"New Directions in Cryptography", IEEE Transactions on Information Theory, vol.22 no.6, pp.644-654, Nov.1976

[10] R.L. Rivest, A.Shamir, and L.Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM, vol.21,no.2, pp.120-127, Feb.1978.

[11] R.C.Merkle, "A Certified Digital Signature", Proc. of Crypto'89, pp.218-238, 1990