International Journal of Security and Its Applications
Vol.7, No.6 (2013), pp.327-334
http://dx.doi.org/10.14257/ijsia.2013.7.6.33

A Study on User Access Control Method using Multi-Factor Authentication for EDMS

Keunwang Lee[1*]
[1] *Dept.of Multimedia Science, Chungwoon University*
113, Sukgol-ro, Nam-gu, Incheon, 402-060, South Korea
kwlee@chungwoon.ac.kr

Abstract

With the recent development of IT society, the value of knowledge information has been focused more importantly. However, the accidents of personal and corporate secrets being leaked frequently happen, and also the damage is getting bigger day by day. The important information of individuals and businesses is leaked or processed by outside attacks or personal mistakes, thus misused, and thereby considerable damage is occurring.

For this reason, the necessity of how to effectively manage personal and corporate information is emerging. This study intends to suggest a method that can protect servers and media information, which requires security. The access control method suggested here uses a way that grants users authority by grade and authenticates users through Two-Factor Authentication method.

This study suggests a way that can reinforce access itself, through Multi-Factor authentication method which falls into users' grade in EDMS(Electronic Document Management System). In addition, when users have access to documents, it identifies users' security grade and the related department, thus limiting the access to the related documents and media. Through the method suggested in this study, we can control access effectively and safely, and can enhance the security of documents and media.

Keywords: *EDMS, Access Control, Multi-Factor, Authentication*

1. Introduction

With IT society getting more complicated and developed these days, the competition between businesses has been tough, and the information of customers or corporate secrets have been important more and more. Information-Processing Technology goes beyond the limitation of time and space, increases the opportunity of getting access to information, and makes it used more easily. Distribution and share of information provides IT service users with convenience under the environment where telecommunication such as Internet has been common.

However, the need to protect information has been emerging since individuals or businesses' important information can be leaked, collected and processed, thus misused by hacking or virus programs, for unjust purpose.

In the existing access method to database, ID/PW authentication is used, or on the intranet PCs, server is directly accessed, and at this point, if ID and PW of a person, whose security grade is high, are exposed by malicious hackers, the relevant server and documents and even

* Corresponding author : Keunwang Lee

ISSN: 1738-9976 IJSIA

media's data can be threatened. Therefore, access to database requires a more secured control[1-3].

To prevent this kind of information leakage accident, this study suggests a way of access control, which can control unauthorized persons' access to documents by incorporating and using the existing authentication method and OTP(One Time Pad) by authority, grant authorized persons the right to keep track of responsibility by recording log data according to security policy, and can quickly counteract it when the accident of information leakage happens.

2. The related studies

In this section, we will look into the studies on access control policy for accessing a system, Two-Factor & Multi-Factor authentication method, and electronic document management system.

2.1. Access control policy

A system's security policy is the directions from upper class, which are used for the design and management of access control system. Generally, they are the basic principles that are expressed by an organization in order to protect the system's resources. In other words, the policy defines the access control principle, whether to allow or reject, according to 5 W's and 1 H.

Access control principle shows the difference of conceptual application, depending on whether it is a closed system or an open system. In a closed system, it allows access to those whose identities are exactly granted, and in an open system, it allows access even if identities are not exact.

As for security policy, it is largely divided into two categories, depending on identity and rule. The access control policy based on identity follows the rule, which is clearly expressed for individuals and groups, who act as an entity or a performer for a specific role. On the other hand, the access control policy based on rule applies all the behaviors made by a certain subject, in order to protect a certain object in the security area [3-6].

2.2. Access control mechanism

Access control system depends on the security mechanism that has security rules and the feature of realizing policies. The role of security mechanism can be regarded as prevention and detection against unauthorized persons, and a powerful authentication mechanism is required to strongly prevent and detect. Authentication of user's identity becomes the base for verifying if a user is an authorized person, in order to control a user's authority for a certain action.

2.2.1. ACL (Access Control List)

ACL defines what kind of work users can do. The maintenance and access control for ACL is not controlled even by Admin, but controlled only by System. Therefore, ACL can be used and realized for the identity-based access control policy, including work-based policy. In addition, ACL has easy expandability since it can add conditions of access control or modify them against a specific entry.

2.2.2. SL(Security Label)

SL is the set of security information that is granted to the objects such as data items or physical resources generally telecommunicated or stored and users. The most common use of SL as access control mechanism is to support with Multi-step access control policy. Every object should have a label that represents the security level granted to itself. When processing an access request, the system determines whether to approve or reject it, by comparing the label attached to an object with the one attached to a subject who requested access.

2.2.3. ID/Password

Though we may not definitely say that access control mechanism based on ID/Password is safe on the network telecommunication, it is being used well since it has a simple structure of function. However, we have much difficulty in keeping and managing password, and especially when a group shares ID and Password together, we have more serious problems. That is, though Password is helpfully used for the purpose of authentication, it needs security for the purpose of access control.

2.2.4. OTP(One Time Pad)

OTP is a password that is valid for a single login session or transaction. OTP Mechanism is a way that server and client generate MAC(Message Authentication Code) and deliver it by a previously determined method, and thus verify its flawlessness and get authentication. Hash functions(MD4, MD5, IDEA, HS5DM, SMD) are generally used to verify flawlessness.

When authentication is needed, token does not need to be physically connected to server since they give and take just one time password, but it works in a way that a person enters the password generated from token, through keyboard. At this point, synchronization of passwords from both sides is the core of this mechanism, and the way to do it includes question/answering method, incident synchronization method and time synchronization method.

2.3. Two-Factor and Multi-Factor Authentication

Two-Factor and Multi-Factor authentication is not a newly made concept. In other words, if we combine one authentication method from ID/Password, PIN or PKI with one or more authentication methods, it is called Two-Factor or Multi-Factor authentication method. This kind of authentication method can be a more powerful authentication than just one type of authentication.

As a simple example, it is the same as we can withdraw money only after we know the secret number of ATM card and bank account if we want to withdraw money from ATM. Here, if we don't know secret number while we have ATM card, or if we don't have ATM card while we know secret number, then it is impossible for us to withdraw money.

2.4. EDMS (Electronic Document Management System)

EDMS (Electronic Document Management System) refers to the system that stores and manages all types of document existing in digital format, makes it easy to get access to information through a single user interface, and makes multi-users in the organization share information and easily utilize it for their work. EDMS is an info-based structure that can accommodate users' request for information and knowledge, standardize and systematize the past ineffective information management systems.

EDMS consistently and systematically manages various types of documents generated from all departments of an organization, from generating, processing, storing, utilizing to disposing documents, throughout their whole life cycle. And it supports all users to be able to get access to them, and it also guarantees the security of whole organizational level through the control system for documents.

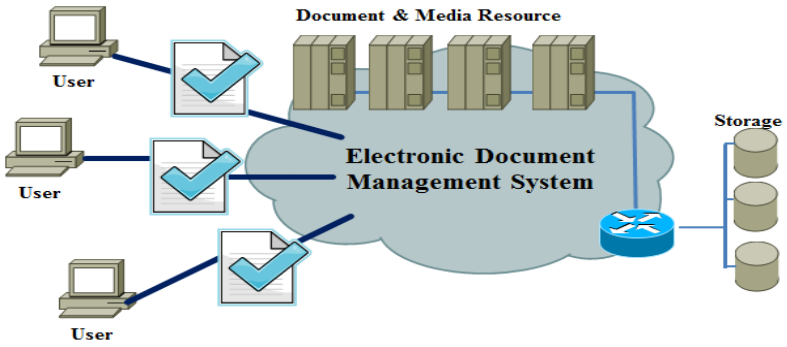

Figure 1. Schematic Diagram of EDMS

3. Access Control System using Multi-Factor

ACAS(Access Control Authentication Server), which is suggested by this study and uses Multi-Factor, consists of AMA (Authentication Management Agent) and FMA (File Management Agent). Though we can additionally apply various factors such as PKI or PIN while authenticating users, we use user ID/Password and OTP only in this study.

If a user accessing to ACAS completes authentication process through IP/Password, the system identifies his identity and grade, generates OTP according to it and then grant it to the user, and then the user can get access to the documents belonging to his grade. As for the document requested by user, the system encodes the document and sends it, by using OTP value falling to user grade and user's public key. Then, the user can view the issued document, using his personal key and the issued OTP value. Figure 2 is the schematic diagram of the whole system.

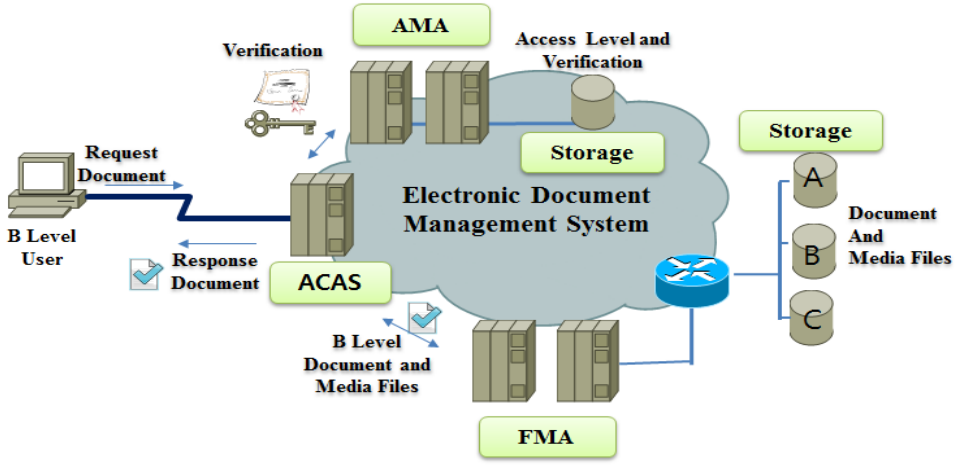

Figure 2. Schematic Diagram of ACAS (Access Control Authentication Server)

A user requests authentication to Server using his authentication certificate, and Server identifies Access Control List of LogDB with that user's authentication certificate, generates OTP value falling to user's grade and sends it to Server, and the user requests the document falling to his grade while having access to File Server by using the issued OTP value.

3.1. Preconditions for user authentication and access control

In the suggested system, it controls user authentication and access, using OTP, which uses question/answering method, and authentication certificate. In regard with this, if we intend to do user authentication and open documents, the following 4 preconditions should be satisfied.

Condition 1: Authentication certificate and OTP issued to user can be used only with the devices users such as PC or notebook computer that users already registered.
Condition 2: User's ID, PW, rank, department and OTP device ID should be registered in advance in AMD, and user ID and device ID should be the only one.
Condition 3: Each file stored at FMA is designated by Security Label.
Condition 4: Though administrator has the right of Top-Secret for Access Control List, he cannot have the right for documents.

3.2. Process of Document registration and Issuance

The person, who provides documents, sign in with his personal key, grants the grade, and then stores them at File Server. Figure 3 shows the process of document registration in the suggested system.

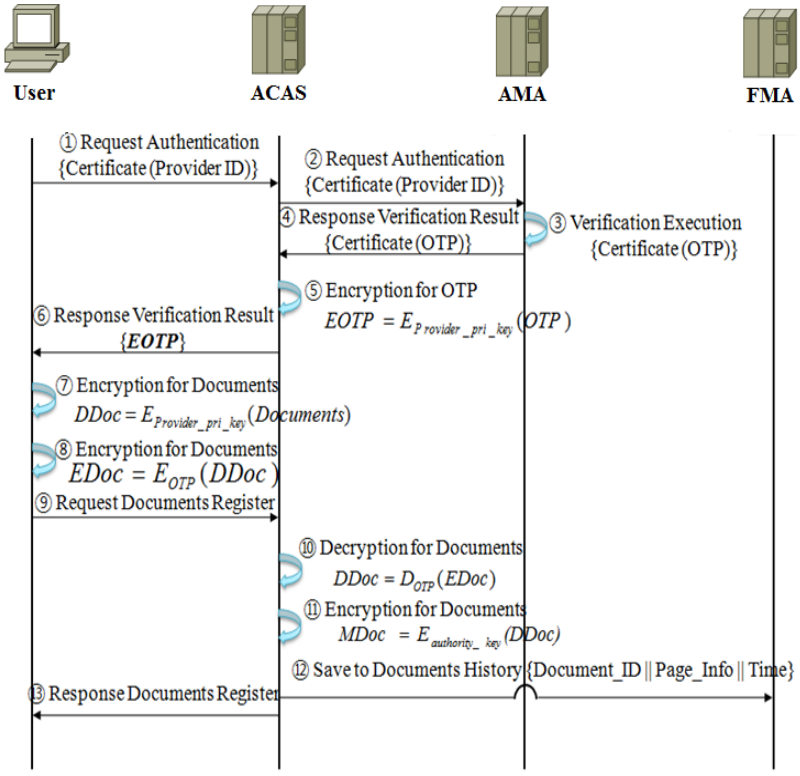

Figure 3. Process of Document Registration

Step 1: User requests access to ACAS with his authentication certificate.
Step 2: ACAS identifies user's grade at Access Control List of AMA, using the user's information who requested access.
Step 3: AS generates Challenge Number, and then generates OTP by inserting the requested Key into Hash Function.
Step 4: It encodes the generated OTP number to user's public key value, and then sends it to the user who requested access.
Step 5: User decodes the encoded OTP value to his personal key.
Step 6: User signs on the document with his personal key, and sends it to Server by using OTP value and encoding the document.
Step 7: Server decodes the document using OTP value, stores it at File Server by using the key falling into the signed document's grade, and then notifies it to the provider.
User gets access to ACAS using the issued authentication certificate, and the document falling into the user's grade is issued to user after checking user's grade. The process of issuing the registered document is as shown in the Figure 4.

Step 1: User requests authentication to Server, using the issued authentication certificate.
Step 2: ACAS identifies user's grade, using user's authentication certificate and passing through AMA's ACL, and then generates OTP value and sends it.
Step 3: ACAS encodes the generated OTP value to user's public key, and sends it to user.
Step 4: User decodes OTP value with his personal key.
Step 5: User gets access to File Server and requests the document falling into his grade.
Step 6: ACAS encodes the document, using the generated OTP value and user's public key, and then sends it to user.
Step 7: User decodes the document, using the issued OTP value and his personal key.

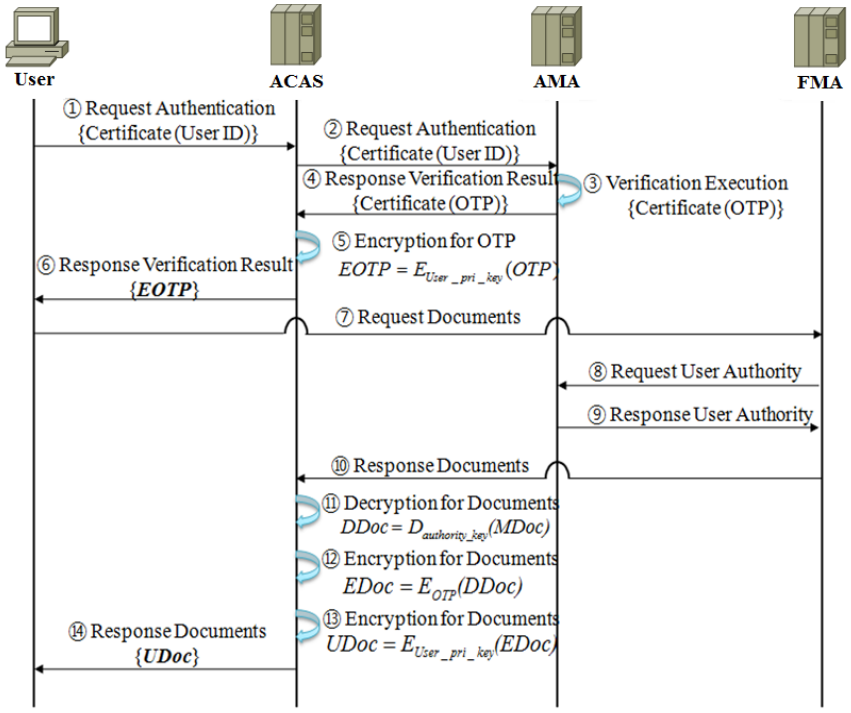

Figure 4. Process of Issuing Document

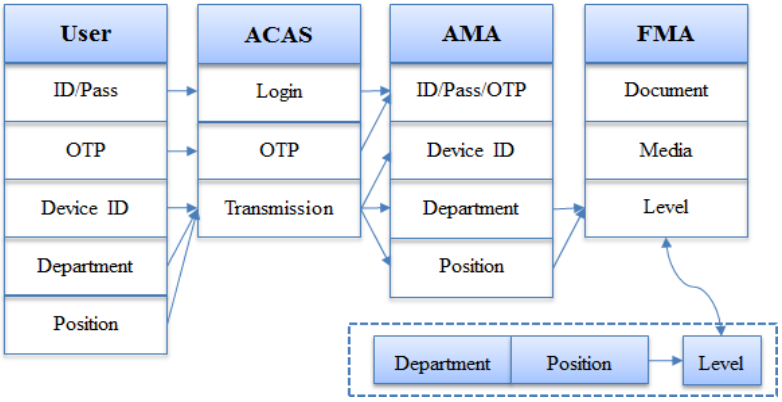

Figure 5. Management of Authority by User

4. Comparison and Analysis

Access control method using Multi-Factor, suggested by this study, uses ID/Password and OTP for user authentication. When we compare the user authentication method with the existing single factor authentication method, it has the strength of excellent security and powerfulness. The results of comparing expense, safety and speed among ID/Password method, PKI method and the system suggested by this study, are shown in the Figure 6.

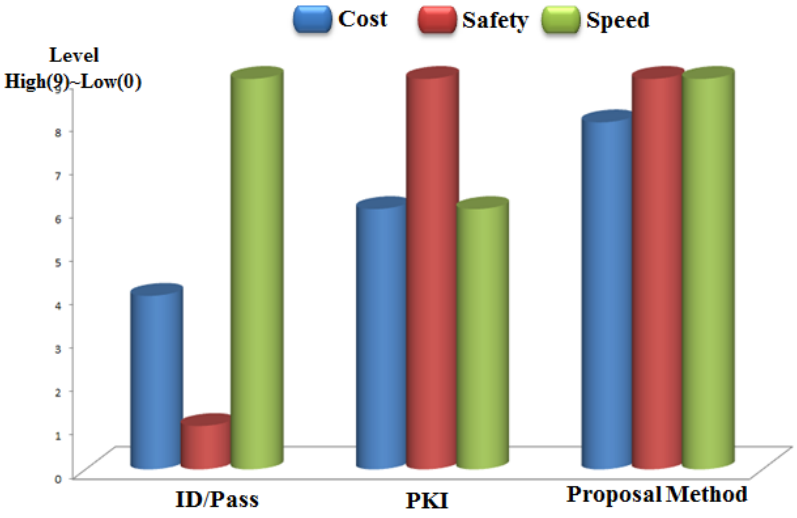

Figure 6. Performance comparison between ID/Pass, PKI and the suggested Method

The above Figure 6 shows the results of measuring 3 factors, for ID/Pass method, PKI method and the method suggested by this study. We obtained the results of measurement, by setting each factor's value to 9 levels and matching them with each factor's item measurement in 9 levels. Among them, the method suggested by this study showed more excellence than other two methods in the aspects of expense, efficiency, safety and processing speed.

5. Conclusion

In user authentication and access control system, Access Control Method using Multi-Factor, suggested in this study, is thought to have more excellence than other authentication-based systems, in the aspects of expense, efficiency and processing speed. And, Access Control Method also shows big difference in regard with safety when we compare the case with other cases using only authentication certificate.

Therefore, even if we don't use PKI system, which uses public key structure, we may be able to apply the most effective access control system with just low expense. From the viewpoint of software, there can't exist a perfect security system, and we need to make security environment stronger. To do this, we may have to provide the further defensive environment, coupled with physical security control at all times.

References

[1] M. Singh, M. Singh Patterh, and T.-H. Kim, "A Formal Policy Oriented Access Control Model for Secure Enterprise Network Environment", International Journal of Security and Its Applications(IJSIA), vol. 3, no. 1, **(2009)**, pp. 1-14.
[2] R. Awischus, "Role-Based Access Control with the Security Administration Manager (SAM)", ACM Workshop On Role Based Access Control, vol. 2, **(1997)**, pp. 61-68.
[3] X. Fu, K. Wu and X. Z. Gong, "Implement Access Control Architecture to Enhance Security and Availability of Cloud Computing Systems", International Journal of Security and Its Applications(IJSIA), vol. 6, no. 2, **(2012)**, pp. 245-250.
[4] M. Su, F. Li, G. Shi and L. Li, "An Action Based Access Control Model for Multi-level Security", International Journal of Security and Its Applications(IJSIA), vol. 6, no. 2, pp. 359-366.
[5] Z. Changyou, C. Yuanda, L. Renfen, L. Yanhua and C. Liang, "An Access Control Mechanism based on Permission Delegation in P2P Network", International Journal of Security and Its Applications(IJSIA), vol. 2, no. 2, **(2008)**, pp. 59-70.
[6] F. Zhao, T. Nishide and K. Sakurai, "Multi-User Keyword Search Scheme for Secure Data Sharing with Fine-Grained Access Control", Lecture Notes in Computer Science, no. 7259, **(2012)**, pp. 406-418.

Author

Keunwang Lee received his B.S. degree in Computer Science from Hanbat National University, Daejeon, Korea, in 1993, and M.S. and Ph.D. degrees in Computer Science from Soongsil University, Seoul, Korea, in 1996 and 2000, respectively. He is currently an Associate Professor in Chungwoon University, Chungnam, Korea. His research interests include multimedia communications, multimedia applications, mobile communications, and multimedia security.

