International Journal of Control and Automation
Vol.7, No.5 (2014), pp.235-246
http://dx.doi.org/10.14257/ijca.2014.7.5.26

A Study of Authentication and Access Control for Library Research System

Jeong-Kyung Moon[1], Jin-Mook, Kim[2] and Bong-Hwa Hong[3]

[1, 2] *Division of IT Education, Sunmoon University*
[3] *Department of Information & Telecommunication, Kyunghee Cyber University*

{[1]moonjk, [2]calf0425}@sunmoon.ac.kr, [3]bhhong@khcu.ac.kr

Abstract

Currently, the changes of computer relation technique are very quick. Specially, the cloud computing development is quick dazzlingly in about field. We have interest about Book Search relational subject in the cloud computing using PC and mobile computational device such as Smart-phone, Tablet, and Ultra-thin book. These devices are showing our general computational environment at least. It cans us to search and play various documents and multimedia data on cloud computing environment devices such as book research, English learning, music play, and movie services. Especially, we have many interests about Library Research Service such as book, music and movie services. If we support to efficient service to user then we must solve to user authentication and device authorization problems. But any similar book search services don't to solve these problems at now. Only they can support to multimedia service or to support user authentication or service authorization service participial. It is very dangerous to cloud computing environment. So we propose to AACLRS that can solve to user and device authentication, service authorization by privilege management schemes. And our proposed system can support various security services such as confidential, integrity, availability and mutual authentication. Additionally, our scheme is very convenience against of existent library search systems.

Keywords: *Authentication, Authorization, Access Control, Privilege management, Library Search System, BRS*

1. Introduction

We are changed by knowledge information techniques. Especially, the cloud computing technique makes more change to us very convenient. So, our life becomes to change digitalized and easy. And the library retrieval and multimedia data retrieval systems are belonging to us more important in some University for digital life [13, 15].

Now, many universities have great multimedia data such as book data and lecturing animation, music, movie and various. But, user only can use in those university to search and play. So, we need that university cooperation and database integral management system for many users can contact and use various information resources usefully [11].

And this system may makes to improve usefulness and to permit search the Library Search System in each university has integration DB. It will be making our information society more easily and efficiently at his homepage using his university account at once [8, 16].

[1] Jeong-Kyung Moon is First author.
[2] Jin-Mook Kim is Corresponding author.

ISSN: 2005-4297 IJCA

Development of information Technology and Cloud services can supply useful to user. And those will make more efficiency to every user. But Cloud service integrates existent computing resource. It includes various security problems in cloud computing environments [1].

Therefore, we must solve access control and user authentication of Cloud services than we will have to free from expected security problems such as confidentiality, integrity, mutual authentication, authorization in ubiquitous computing environments. Also, necessity of device identity and user's grade access will be great [4, 5].

So, we propose AACLRS (Authentication and Access Control for Library Research System) that is called ANDA2CS (A Noble Device Authentication and Access Control System for Library Search System) by our older study. It can provide different access control by user's grade and device authentication with user identity service. And it can support to Authorization using PMI (Privilege Management Infrastructure) technology [8].

2. Related works

2.1. BRS (Book Retrieval Services)

Since the 1960s, search information for books that is prospering and decay in the library effectively and research of BRS went ahead to improve efficiency of book lending. In this way, BRS is literary field that exist to improve efficiency in book search very for a long time [2].

Lately, development of Information communication technology environment make that to book search is very fast by make XML documents with information of book and structure of books [3, 4]. Also, it can search and share information about store a book or digital data effectively using logical configuration of XML document. BRS (Book Retrieval System) extends search function in itself. It can possible to search by structure retrieve, mixing search, attribute search, and content retrieval using computer and Internet technology [1, 5]. Figure 1 is expressing structure of system that can define document structure using XML and after store on computer internet by connection intermediate in remote user book information that wish to find search [7, 9].

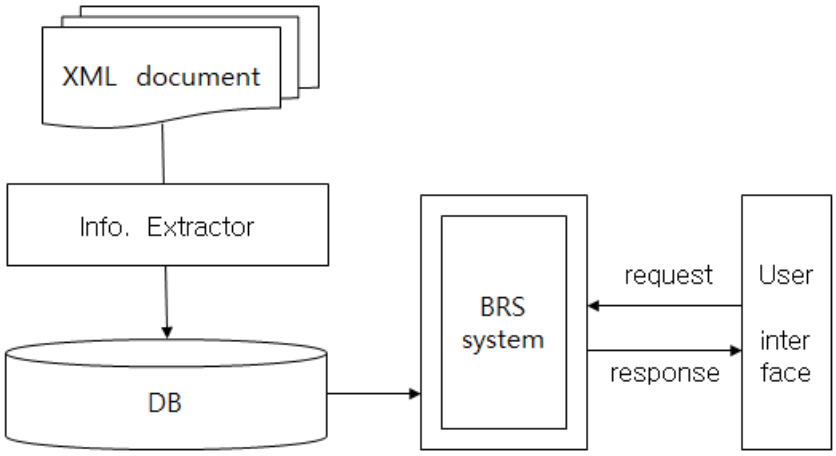

Figure 1. Structure of BRS

Well, Figure 1 Showed BRS's structure. BRS creates and save the XML document by abstract to attribute and frame information of each document. And when user want requires, BRS can transmits without damage information that searched in DB.

2.2. Authentication Services

Authentication services can support to identification and right by user id and password or more difficult methods. General authentication method is user id and password check method. But this is very easy and it has threat to attacker [15]. So, now many researchers make more difficult and convenience authentication services such as Kerberos, PKI and PMI.

2.2.1. Kerberos

MIT research team develops Kerberos protocol within Athena project. This is a international standard by RFC-1510. This is Token based authentication protocol. Figure 2 shows Kerberos easily.

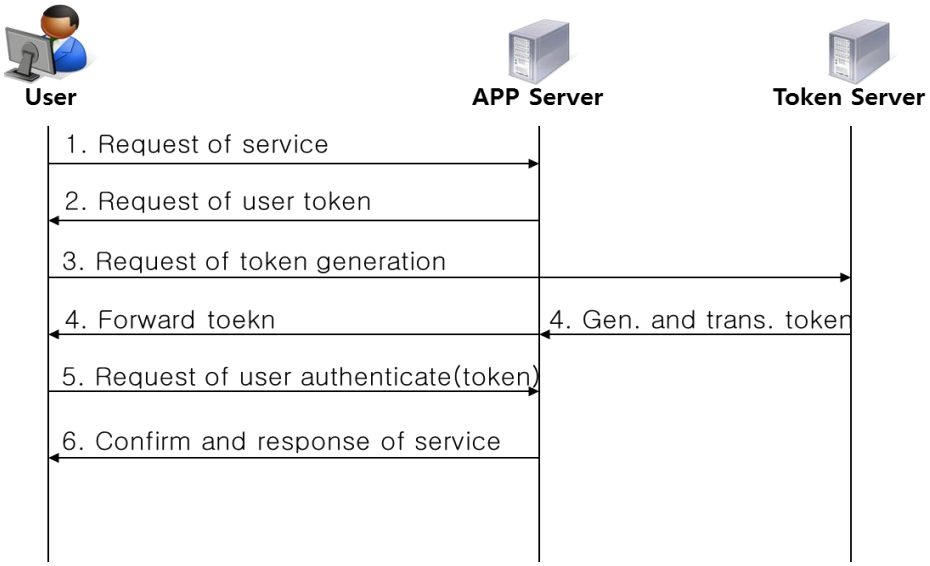

Figure 2. Structure of Kerberos

Kerberos have 6 steps. First, user request service to Application server then Application server request of user token to user. Second, user request of token generation to token server then Token server make a token and Transmit to user it. Third, user request user authentication with token to Application server then Application server checks user token. If user authentication token is right then Application server response to user with service. This is a simple Kerberos procedure.

Kerberos protocol can support authentication to user by token with simple procedure steps. This protocol was developed by international authentication standard. But this protocol has various threats. Because this protocol only support to only simple authenticated process. But this protocol can't support Public Key based authentication. So, now advance authentication protocol must solve difficult and complex jobs for authentication.

2.2.2. PKI

PKI is an authentication international standard by Public Key based schemes with X.509 Ver. 3. This protocol has 7 steps process for authentication based on public certificate. Figure 3 shows it simply.

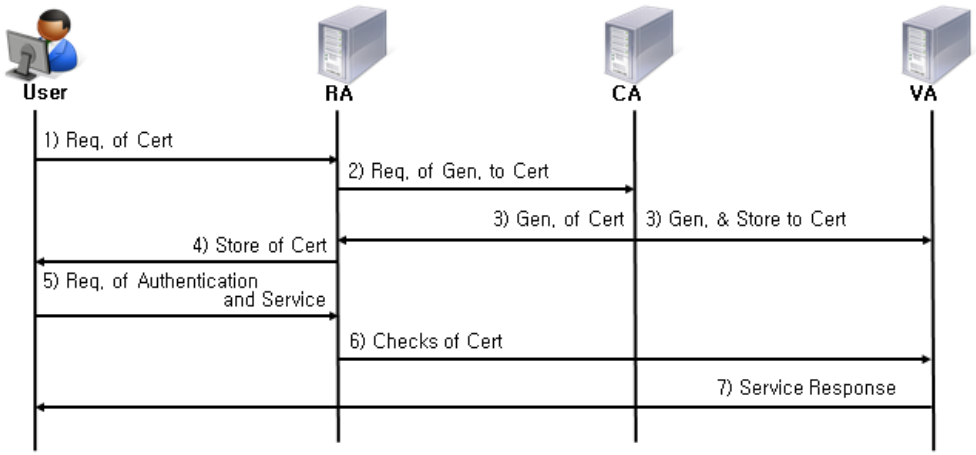

Figure 3. Structure of PKI

First, user wants certificate generation by RA. And user request certificate to RA then RA request certificate to CA instead of user. Second, CA make certificate and store itself. And CA transmits certificate to RA and VA. This agent store certificate user-certificate.

Third, user request authentication and service to application server. Then VA want checks user authentication by user certificate. If user certificate is right then VA allow user wanted service.

2.2.3. PMI

PMI (privilege Management Infrastructure) is authentication service on various authentication and authorization service. PMI is international standard using privilege schemes. It can support authentication base on Public Key schemes and authorization by privilege on data structure with expand fields [16].

It includes LDAP and X.509 Ver. 3 expanded certificate. If user wants service then PMI agent checks user-id, password and certificate by LDAP. And application server checks service-id and service-permit by user authentication information. If user-id, service-id, service-permit is right then application server support user wanted services to user. But these are doesn't right then application server don't support to user wanted services [6, 14]. Figure 4 shows PMI.

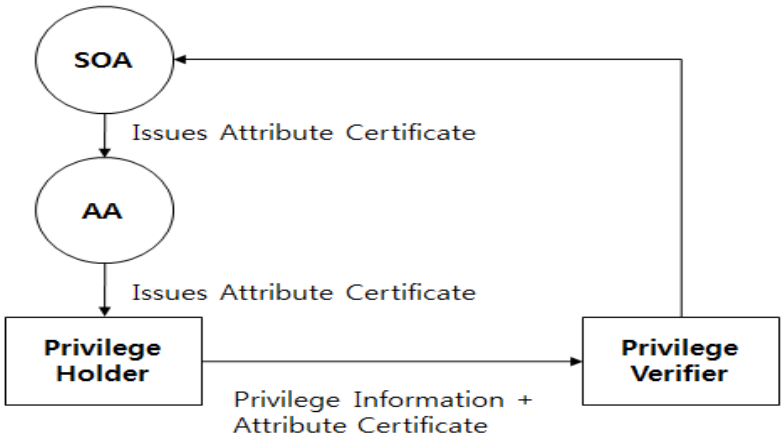

Figure 4. PMI

2.3 Authorization Services

Authorization services support different service to user by user having grade about service. Many authorization services were developed by security developer. It based on access control rule or permits [15].

Our proposal authorization services based on PMI expand fields. It fields include user access control permit information. Each permit allows user access control.

3. AACLRS (Authentication and Access Control for Library Retrieval System)

3.1. Architecture of our proposal system

AACLRS does to search fast and safety sharing storage, a managing book or information about digital data in several colleges unlike thing which existent BRS could store and search a book or digital data information superlatively. In this time, AACLRS use a attribute certificate based on PMI that can approach to BRS according to user's grade who want to search book information as is different. Figure 5 shows our proposal system.

In figure 5, user 1 want research his wanted multimedia data for play on his PC to application server 1 that is BRS in our university. In this time, application server 1 search user1's authentication information and if his authentication request if right then application server 1 request server 5 to total authentication and authorization service.

AACLRS is server 5. This server checks user authentication information and authorization information then if these information's are right then allow his wanted service to server 1. But application server 1 don't have user 1 wanted service information then server 5 research user 1 wanted service information using LDAP. If server 3 has user 1 wanted service information then server 5 mutual authentication checks between server 1 and server 3.

Application server 1, 2, 3, 4 have mutual authentication rule older time. So, they can support to mutual authentication service in this network group. And another application server want insert this network group then server 5 checks it's mutual authentication service support ability.

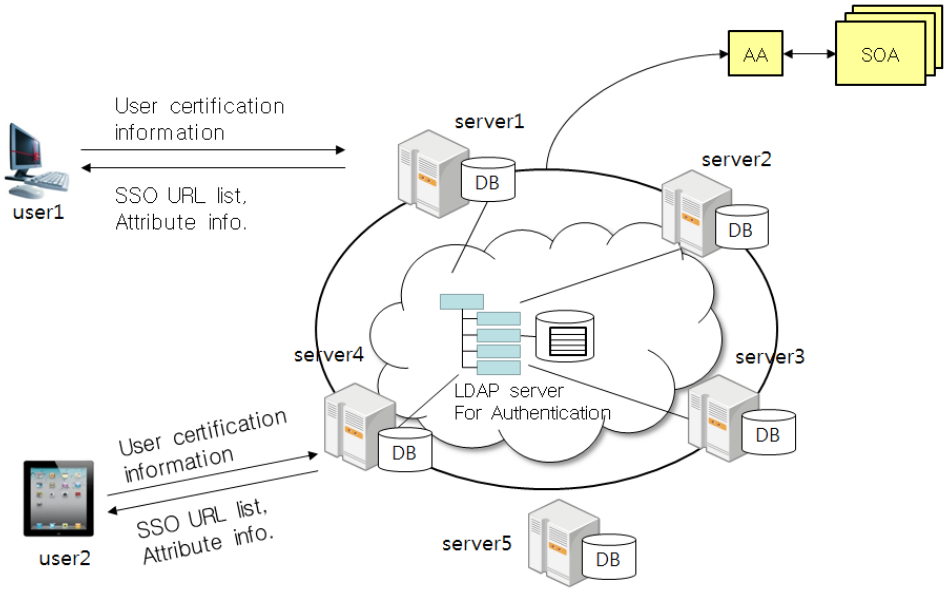

Figure 5. Architecture of AACLRS

Moreover, our proposed system supposes PMI that can use Delegation Model. For this, we give different 5 grades to user in AACLRS. It can user approach our system by differential privilege. Also, we propose that each sever can certificate mutually in our proposed system. Then, even user included book search server is different. Each user is available login to book information retrieval servers by oneself mutually. So, we applied SSO function for AACLRS. Figure 4 is displaying AACLRS's system structure that we propose in treatise. As appear in Figure 4, user1 can join and use to server1, and server2, 3, 4 using SSO service. And user 1 searches of all data within 4 colleges are allowable digital data. User1 was update to certification server 1's DB periodically. So user1 can do something.

If user1 passes own token and PMI attribute information to authentication server than authentication server examines this and inform certification availability to user1 and server1. If examination result agrees, server1 allows access about information that want according to user1's attribute grade. Similarly, if user1 requests to search information connecting to server2, certification server admits so that can search attribute information about user1 that is storing by oneself and use allowed information according to user1's attribute grade. In this way, each server1, server2, server3, and server4 can examine whether have access about user1dl confidence to certification server whenever user1's use request happens, have some attribute certificate and admit according to access possibility availability and attribute grade.

Our data structure has many expanded field with attribute certificate by expanded field in X.509 Ver. 3. Table 1 shows our proposal data structure using PMI information structure that IETF proposes, and use Delegation Model by attribute certificate distribution way. Define Attribute field and Extension field information of these fields as following.

Table 1. Profiles of privilege certification

Version	Holder	Issuer	Signature	Serial #	AttributeCert ValidatePeriod	Attributes	Issuer UniqueID	Extensions
Version of Cert.	Who save	Who generate	Digital sign	Serial Num. of gen.	Period check result of AttributeCert	Various attributes This field use in our paper for user grade	UniqueID for Issuer	Extension for another information

First field include version information. This field includes information X.509 version data. Generally, we use X.509 ver. 3. Second field include Holder information. Holder means this profiled data owner. Example, this paper writer is holder. And Issuer field include profile generator data such as KISA in Korea. Signature field is electric signature information list by holder and issuer. Serial number field include issuing number by issuer. Attribute cert validate period field includes validate period information in this time. User and application server must checks this field for freshness.

Attribute field include privilege information such as user can read, write, modify and so on. Some application server can issuing user permit about wanted service to user. So, we this field is very important field. We propose 5 grade attributes at each BRS server. Our proposed user grade level as following:

① Grade 5: searchable book title and summary

② Grade 4: searchable book title and Read book

③ Grade 3: searchable book title and Read multimedia-content

④ Grade 2: searchable book title and Download multimedia-content

⑤ Grade 1: searchable book title, Download and Edit multimedia-content

Each application server must checks attribute field for right service to user by user haven grade information.

And we support the information about user privilege in extension field on ESAM. It is following:

① Expired time of PMI certification

② Server information(name of server, group name of server,

Server certificate information)

③ Notification that using privilege certificate

④ Policy about privilege

Extended attributes field and extensions field in structure to be attribute certificate professional par that appear before in proposal system. In addition, establish user grade and input valid server information and did differentiation by this so that can run done access control and user authentication.

3.2. Procedures of AACLRS

AACLRS can support user authentication by ID, PWD and certificate information using X.509 based certificate. And AACLRS can support service authorization by PMI schemes. Figure 6 shows AACLRS procedures to authentication and authorization using our proposed schemes.

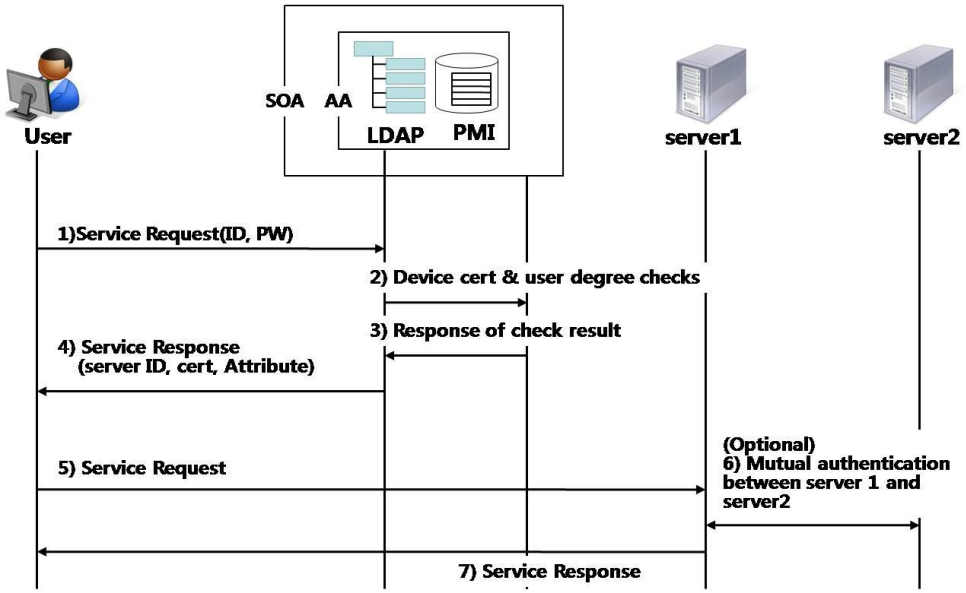

Figure 6. Procedure of AACLRS

If user want that search service by book title by server 1. First, user sends to authentication server ID and PW. Then authentication server checks user's device certificate and user degree by user-id and password within mutualized authentication and authorization server using LDAP protocol. Second, mutualized authentication and authorization server checks user wanted service possibility and certificate information. If user have right certificate information and authorization grade then authentication server response of checks result to user. Third, authentication server transmits service response to user. This packet includes server-id, server-certificate and user-attribute field information.

Next, user want service request to server 1 or 2. If between server 1 and server 2 can support to user wanted service then checks mutual authentication and response to user. And some server response service to user.

Procedures of proposal system have 7 steps. But we will explain to 4 steps simply. It is as following:

1) If user connects to server1 than server1 requests certificate about user to certification server automatically (this time, if user use mobile communication device, server1 request to device certificate to authentication server).

2) Authentication server can receive user attribute information and SSO server list that is stored in LDAP directory. If sever is delegation model that is not registered to AA, AA search and decide use permission availability whether is user who is registered to SOA's server.

3) Coming server1 and server2, included server can request book search or multi-media animation by user's grade.

4) After user finishes use permission, he has different service according to own attribute grade. Also, each server divides and connects 5 grades by user who approach to book search.

For front, plan to examine and ready solution in reply and apply to implementation about problems that can happen actually about mobile device certification and so on embodying system. Therefore, explain straightforwardly about part to process between AA and SOA in midway in figure

4. Evaluations

As appear in Table 2, we analysis to existent authentication and authorization service against of our proposed system. Generally, Kerberos protocol has fast speed because it use token authentication method. It is very simple authentication way. But our proposed system has Middle speed because AACLRS more complex process.

Table 2. Analysis of our proposed system

	Kerberos	PKI	AACLRS
Authentication	Token	Certificate	Certificate
Authorization	None	None	PMI
Confidentiality	None	None	Possible
Integrity	Slow	None	Possible
Speed	Fast	Very Slow	Middle
Complexity	Simple	Complex	More complex

4.1. Confidentiality

Example, Kerberos can't support confidentiality service between book retrieval server and user because this protocol is only authentication protocol. So, if user wanted research data about book then server can only transmit wanted data. Belonging to data transmit to user, if some attacker can cheat this data. This is a very critical security problem.

But in our proposed system, we can support confidentiality service by encryption algorithm. So in AACLRS can guarantee confidentiality to user. This is a very important thing. Our proposed system can solve Man-in-the-Middle-Attack by this scheme.

4.2. Integrity

In our proposed system, user must have signature for request service and so on. And various servers have signature too. When user want data transmit, his signature transmit to service provide server. And service server response service request result with server signature.

So, user's and server's signature include communication data packets. This information can support integrity service. Some people try to deny to service request to service provide server then server checks user's signature and evaluate his wanted information. If some people want book retrieval service to server 1. But he denies to this situation, then severs

check transmitted data and extracts user signature field and his privilege information. And transmit authentication server to user dis-right or deny action checks.

4.3. Special authorization service

In AACLRS, if user wants that cheats his service grade level and transmit to server for service support. First, authorization server checks user have authorization data in mutual authentication and authorization server. And if user authorization data is not correct, service provide server don't support it to user. And alert to user and service servers.

5. Conclusion

AACLRS have differential characteristic because this system can support to various university library make integration book search service and management. So, our proposal system can provide more effective book search result and rapid response time. And when user want to search a book using a mobile device than our system provide to hardware certification of mobile device that can solve various security problems before the process. Also, propose scheme should be decide the user authentication and access control by user privilege grade based on PMI.

Therefore, we were suggested AACLRS that will support to mobile device certification and user authentication by user's privilege grade for book retrieval or multi-media services. Our proposed scheme design and implement. For example, we make a simple action supported program that can use for book search or multi-media data access or download by user grade differently.

By the result, our proposed system that is suitable certification with mobile device and available mutually user authentication on various server group in cloud computing environments. And we know that user get possibility within cross certification using delegated model for user authentication.

AACLRS based on SSO, So, it may be offer convenience because it can use every cross certified sever. And it offer to safety as like upper.

We were suggested AACLRS that is device certification and user authentication system. It is based on attribute certificate schemes in this paper. As well as, we select a typical service that is library search system. And we will more study to various cloud services after future work. And we are going to evaluating and analyzing about our proposed system.

Acknowledgements

This article is a revised and expanded version of a paper entitled "An Noble Device Authentication and Access Control System for Library Search System" presented at International Symposium on Advanced and Applied Convergence held on November 14-16, 2013 at Seoul, Korea.

References

[1] D. Shin, H. Jang, and H. Jin, "BUS: An Effective Indexing and Retrieval Schem in Structured Documents", ACM, **(1998)**, pp. 235-243.
[2] C. -B. Son, B. -Y. Lee and J. -S. Yoo, "Design and Implementation of a XML Document Retrieval System Using the BRS/Search System", Journal of Korean Society for Internet Information, vol. 2, no. 2, **(2001)**, pp. 1-13.
[3] J. -K. Moon, J. -M. Kim, H. -R. Kim and H. -Y. Jeong, "Easy and Secure Authentication Method using PMI", Applied Mechanics and Materials, vol. 281, **(2012)**, pp. 86-89.

[4] C. Bayliss, R. O. Sinnott, W. Jie and J. Arshad, "The Design", Development and Application of a Proxy Credential Auditing Infrastructure for Collaborative Research, E-Technologies, Transformation in a Connected World, Lecture Notes in Business Information Processing, vol. 78, part 6, **(2011)**, pp. 211-226.
[5] D. W. Chadwick and A. Otenko, "The PERMIS X.509 role based privilege management infrastructure", Future Generation Computer System, Elsevier, **(2003)**.
[6] T. Howes, M. C. Smith and G. S. Good, "Understanding and deploying LDAP directory services", Pearson Dducation Inc., **(2003)**.
[7] C. S. Spahiu, L. Stanescu and M. Brezovan, "Fast Information Retrieval using Indexing Techniques", Frontiers in Artificial Intelligence and Applications, vol. 254, **(2013)**, pp. 89-98.
[8] J. Kyung, J. -M. Kim and B. -H. Hong, "An Noble Device Authentication and Access Control System for Library Search System", Proceedings of the 1st International Symposium on Advanced and Applied Convergence, Seoul, Korea, **(2013)**.
[9] T. Dao, S. -D. Ron and J. A. Thom, "An indexing scheme for structured documents and its implementation", Proceedings of the 4th International Conference on DATABASE Systems for Advanced Applications, Melbourne, Australia, (**1997)**.
[10] W. Chin, Y. -J. Roh and K. -D. Kim, "Mobile Book Search System Using WiBro and Voice Information Technology", Proceeding of ICEIC2008, Tashkent, Uzbekistan, **(2008)**.
[11] L. Gao, S. Wang and J. Chen, "Multimedia Information Technology Application in Image Retrieval", Proceedings of the 2012 International Conference on Cybernetics and Informatics, **(2012)**.
[12] C. Zhang and S. Zhan, "Research and Implementation of Full-Text Retrieval System Using Compass Based on Lucene", Proceedings of ICCEAE2012 AISC 181, **(2012)**.
[13] X. Liang, S. Li, C. G. Wei, J. Ma and Y. Luo, "Unity Retrieval Technology of Universities Heterogeneous Data, Proceedings of Informatics and Management Science III", Lecture Notes in Electrical Engineering 206, **(2013)**.
[14] S. W. Parkinson, "Method for issuing attribute certificate from an LDAP entry", U.S. Patent, **(2011)**.
[15] J. Vijayan, "Hackers are defeating tough authentication", Gartner warns, http://www.computerworld.com, **(2009)**.
[16] M. -H.Kang, "PMI: Privilege Management Infrastructure", Future System Research Paper, FS-TR02-01, **(2002)**.

Authors

Jeong-Kyung Moon

She received the B.S degree in Department of Horticulture from Paichai University, Daejeon, Korea in 1993 and M.S degree in Department of E-Commerce from Dankook Univerity, Cheonan, Korea in 2006 and Ph.D. degree in Department of Computer Science and Engineering from Kongju National University, Cheonan, Korea in 2013. She is a Lecture in the Division of IT Education in Sunmoon University currently. She's research interests include information security, cloud computing, library search system, and authentication schemes.

Jin-Mook Kim

He received the B.S and M.S degree in Department of Computer Engineering from Paichai University, Daejeon, Korea in 1998 and 2000 and Ph.D. degree in Department of Computer Science from Kwangwoon University, Seoul, Korea in 20006. He is an Assistant Professor in the Division of IT Education in Sunmoon University currently. His research interests include information and network security, ubiquitous computing, RFID, sensor network, cloud computing, and various authentication and authorization schemes.

Bong-Hwa Hong

He received the M.S. and Ph.D. (major in Computer Architecture) degrees in Electronic Engineering from the Kyunghee University in 1992 and 2001 and Ph.D. degrees in Education from Comberland University, North Carolina, in 2009. From 1997 to 2004, he had been an Assistant Professor in Dept. of computer science at Semyung University, Chechon, Korea. He also had been an Associate Professor in Dept. of Information and Communication of Kyunghee Cyber University, Seoul, Korea from 2004 to 2009. Currently, he is working as an Associate Professor in the Information and Communication, Kyunghee Cyber University, Seoul, Korea. His research interests include Computer Networks, Cyber Education, Digital Contents, Ubiquitous computing.