International Journal of Security and Its Applications
Vol.7, No.6 (2013), pp.21-30
http://dx.doi.org/10.14257/ijsia.2013.7.6.03

A Survey on Security Threats and Security Technology Analysis for Secured Cloud Services

Changsoo Lee[1], Daewon Jung[2] and Keunwang Lee[3]

[1]*Dept. of Computer Science, Soongsil University*
Sando dong, Dongjak-gu, Seoul, 156-743, South Korea
[2] *R&D Strategy Department, The Attached institute of ETRI*
P.O.Box 1, Yuseong Daejon, 305-600 South Korea
[3] *Dept. of Multimedia Science, Chungwoon University*
, Sukgol-ro 113, Nam-gu, Incheon, 402-060, South Korea
[1]*powerofmicro@naver.com,* [2]*dwjung@ensec.re.kr ,* [3]*kwlee@chungwoon.ac.kr*

Abstract

In recent, various types of cloud services such as Web-based cloud and mobile cloud that can store and access documents and multimedia files from a wide variety of client environment are getting rapidly increased. However, the problem is that if a network failure or a security failure occurs due to an intended or unintended accident, we would experience considerable damages. Since cloud services have high portion of virtualization that implies one of the physical hypervisor platforms operating on more than two organizational data, the risks are always present in cloud services at the aspect of security issues. In this paper, we analyze the security threats and security technologies for secured cloud services. We also provide the security requirements for cloud services which help to make a research direction to the new types of security threats.

Keywords: *Cloud Computing Service, Cloud Security Analysis, Virtualization, Network Security, Information Security*

1. Introduction

In most recent three years, the biggest issues in the IT environment are virtualization, cloud services, pand big data analysis. Virtualization is usually used for implementing many of cloud infrastructures. Infrastructure clouds are able to provide computing resources that are logically virtualized and the storage resources that save the images, video, and data over the internet. In recent, with the development of the IT environment, resilience on IT in the business has been rapidly raised so that we also increase the cost of investment and maintenance. Cloud services are collections of a variety of technologies and services and have the characteristics such as resource efficiency through virtualization and energy efficiency and reusability. Accordingly, from the investigation of Gartner, it is expected that the cloud service markets seems an annual growth at a rate of 18.9%, and it will achieve 1,768 billion dollars markets.

As shown previously, the cloud services are getting popular and receiving a lot of attention in recent years. However, research on cloud service security is not enough to cover this area. Most existing the security for the cloud service only provides a limited service for specific cloud services so that it is difficult to conjunct with the security features of other cloud services. Also, as the cloud services have different security characteristics, it does not support

ISSN: 1738-9976 IJSIA

all cloud services. Therefore, there is a need for an effort on surveying security and privacy issues in cloud services and establishing secure and reliable cloud services environment [1-4].

In this paper, we analyze the security technologies for establishing secured cloud computing environment. Section 2 analyzes the recent security threats in cloud services. Then, we provide the analysis of security technologies for cloud services in Section 3. The requirements for cloud computing security are followed in Section 4. Finally, we conclude this paper in Section 5.

2. Security Threats to Cloud Services

Security threats to cloud services inherit the existing IT environments. Also, depending on the cloud characteristics, the new types of threats to data, virtualization, mobile, and data center have been increasing. In this section, we provide the security threats to cloud services happened in the area of cloud service management.

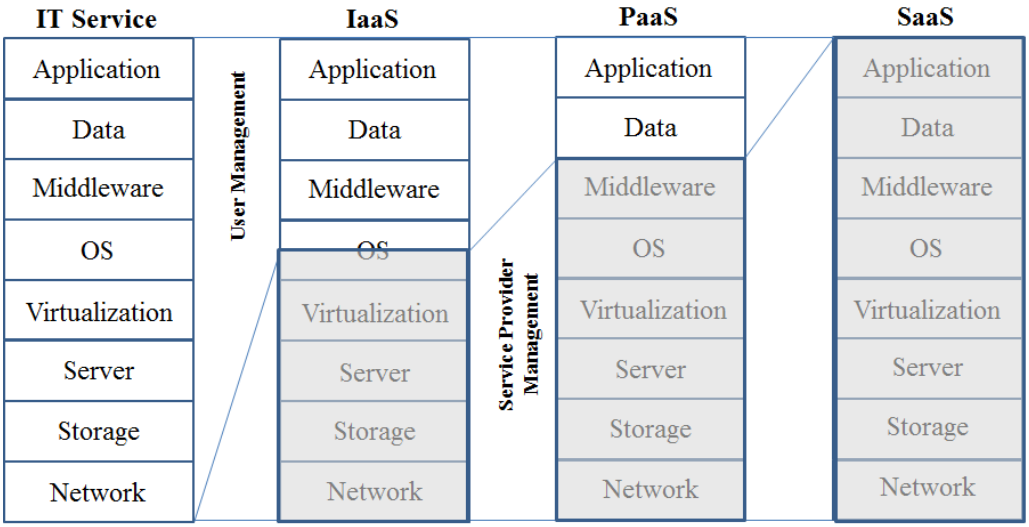


Figure 1. Cloud Service Management Areas

2.1. Security Threats for the Service Provider

2.1.1. Hypervisor Attacks: Since the hypervisor has vulnerabilities to the attacks, the attackers can make a successful attack for obtaining administrative rights and disclosing information by using the hypervisor vulnerabilities. If the attackers obtain the administrative rights of the virtual machine, they can get the applications of users and the information of users. Furthermore, they can attack the other virtual machines as the second attack route in the same physical system. The attacks using hypervisor vulnerabilities are known as integer signedness error and communication components vulnerability between the guest and the host OS. First, integer signedness error is an attack using the vulnerabilities for checking the validity of the permission level. Second, the attack using the communication component vulnerabilities between the guest and host OS is acquiring access rights by making a heap overflow in the process of interaction and initialization of the communication components [5].

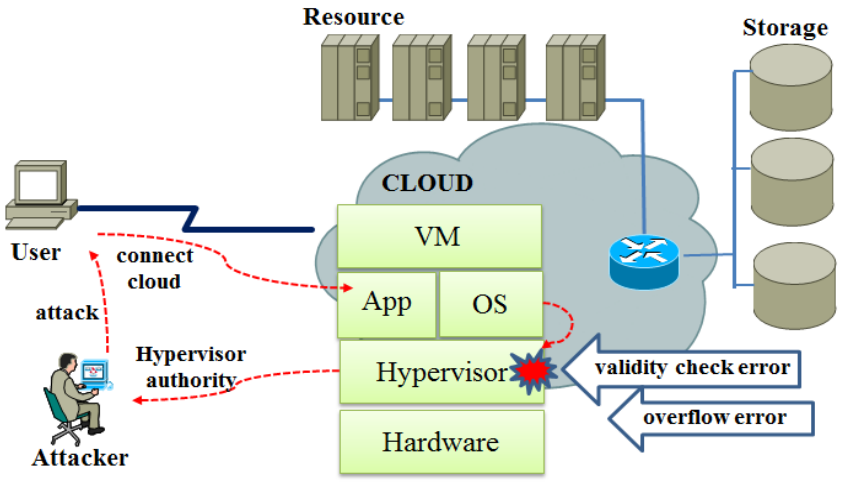


Figure 2. Attack using Hypervisor Vulnerabilities

2.1.2. OS and Web Vulnerabilities Attack: Attackers may attack the user PC that is vulnerable to the malware infections to acquire the right of users connected to the cloud service. Then, they try to find the web vulnerability for the attack to the virtual machine. Also, they perform activities of infection and spread of the infection by the activity of illegal communication between the virtual machines. We also can use the vulnerabilities when API in OS calls I/O control in the devices, finally leading to getting OS authority. Figure 3 shows one of the attack methods using the vulnerability of the OS and user authorities acquired.

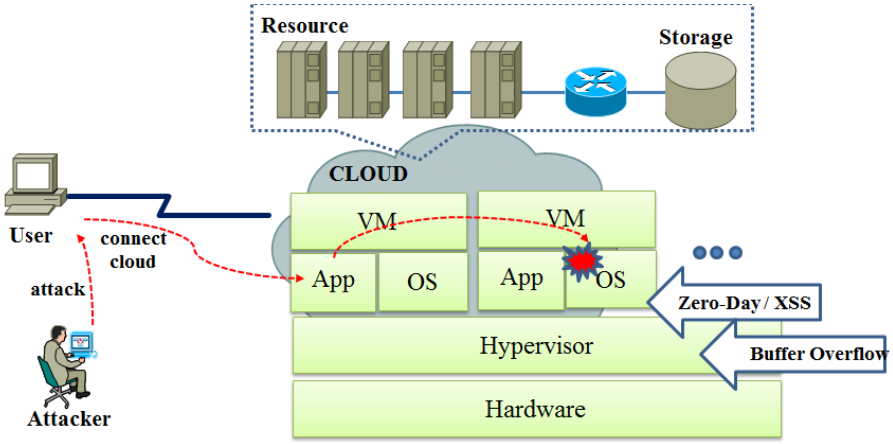


Figure 3. OS and Web Vulnerabilities Attack

2.1.3. RootKit Attacks: Once attackers acquire the user authority that can connect to the cloud service, they install the RootKit in the virtual machine. RootKit can attack from virtual machine controlled by the internal attacker other virtual machine and hypervisors. In the case that the attackers acquire the memory access authority, they are able to monitor all the virtual machine's memory such that it becomes a very big threat [6].

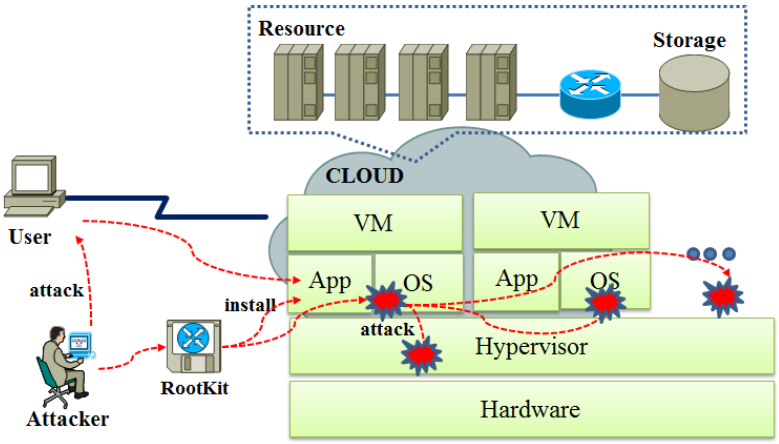


Figure 4. RootKit Attack

2.2. Security Threats for the Users

2.2.1. Changing User Information by Sniffing: In order to access SaaS service, which is one of the cloud services, it is necessary to perform authenticating user ID and password. At this time, when this information passes to the server-side while username and password information is not encrypted, user account information can be stolen by the sniffing attacks to user session. Attackers can steal the user data, authentication information, and financial information.

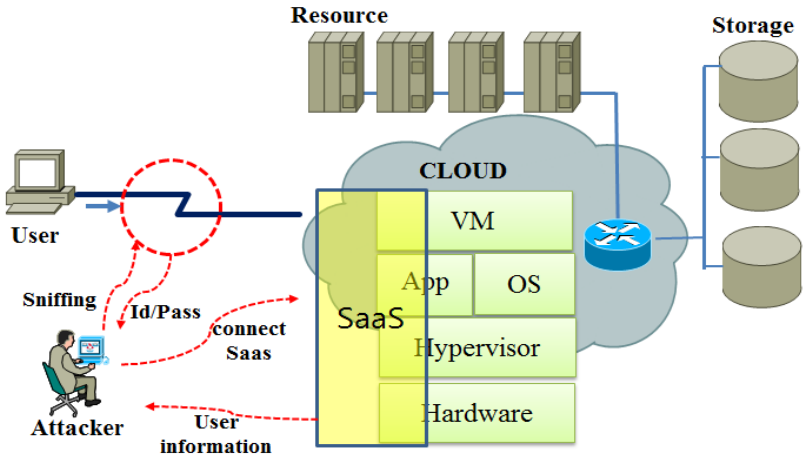


Figure 5. Changing User Information by Sniffing

2.2.2. Changing User Information using Hijacking: Hijacking is the method to steal the session ID granted to use the SaaS service in HTTP and TCP networks. With this session ID, they can use the normal cloud services. In the case of DLL hijacking, it is also possible to steal SaaS account during the loading process when a program run by the user request the DLL from OS [7].

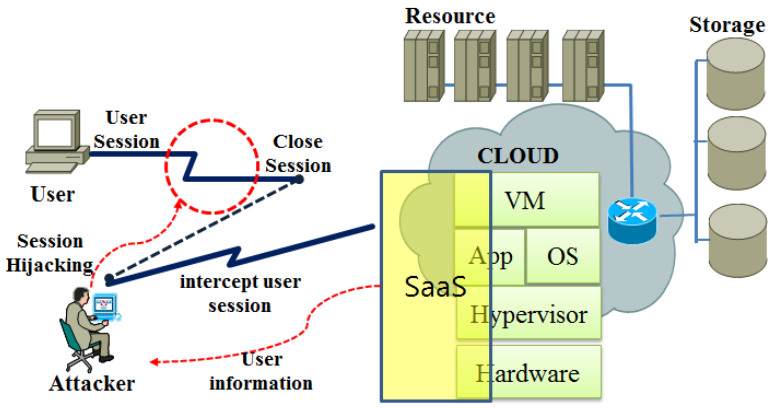


Figure 6. Changing User Information by Hijacking

3. Security Technologies for Secured Cloud Services

Because cloud computing technology that can provide a new user centric service is an extension version of the IT technology, security technology has not been characterized well. We believe that cloud computing security threats are the similar to those that occur in the existing IT environment such that security technology is also possible to apply to each security component.

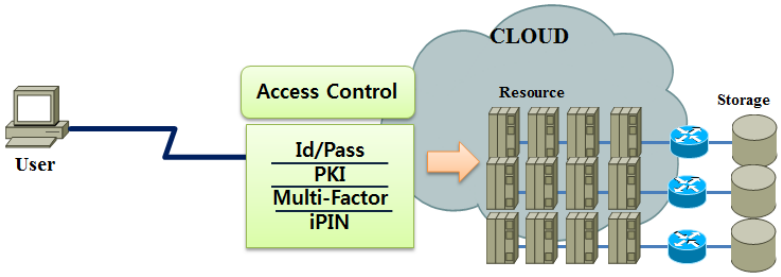


Figure 7. Access Control and User Authentication

3.1. Access Control and User Authentication

Access control and user authentication technologies are the most representative security technologies for platform and cloud computing security. Access control technology is used to protect the resource by classifying the grades or jobs to access their resources. DAC(discretionary access control), MAC(Multi Access Control), and RBAC(role based access control) are typical access control technologies. DAC is a method to give a granted access based on an individual user or group identifiers. It also gives a same level of authoritiy to other users. MAC gives vertical and horizontal access rules for system access. Note that this method is the widely used, mainly in the military or government agencies. In the RBAC method, some of the authorities given to the root user are allowed to give the specific users called role user. In Figure 7, user access control is determined by the rules of cloud system. In terms of user authentication, Id/Pass, PKI, Multi-Factor, iPIN, and OPT are widely used.

3.2. Network Security Technology

With the development of IT technology and the spread of Internet, as the security threat increases, network security technologies also have been improved. Leading technologies are SSL for ensuring the confidentiality of communication, IPsec, VPN, and IDS/IPS, Firewall, and DDoS prevention techniques.

3.2.1. SSL(Secure Socket Layer): SSL not only applies to the session layer, but also ensures the safety of the protocol for FTP, Telnet, and Http in application layer. Therefore, it ensures server authentication, client authentication, and message confidentiality. This SSL supports HTTP(HTTPS:443), TELNET(TELNETS:992), POP3(POPS:995), FTP, and NNTP.

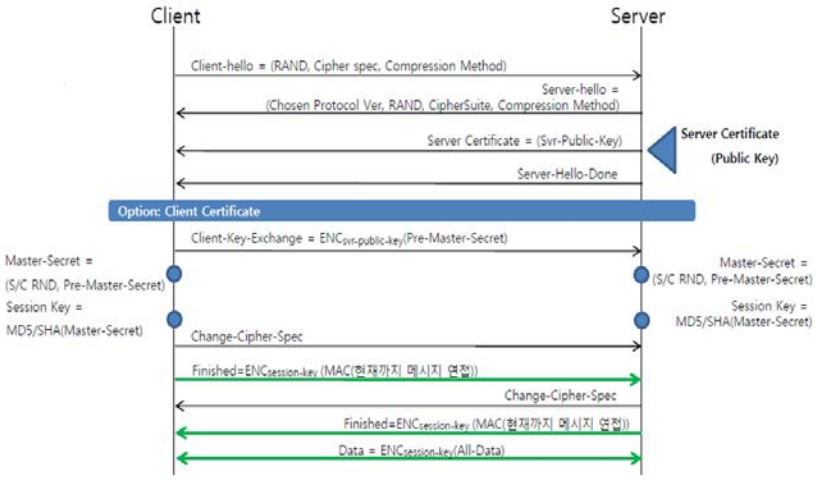


Figure 8. Flow for SSL Protocol

3.2.2. VPN(Virtual Private Network): VPN is a technology that enables public network to use like a dedicated private network by using tunneling and encryption technology. With this VPN technology, we can expect following things: i) reducing the cost for building private network, ii) circuits fee reduction, and iii) increasing data reliability. VPN is divided into two parts: one is tunneling technology, and the other one is encryption technology. The tunneling technology used in VPN means that it forms a tunnel from the starting point to the end point in order to send and receive information through a virtual tunnel, which is not affected by outside of the network.

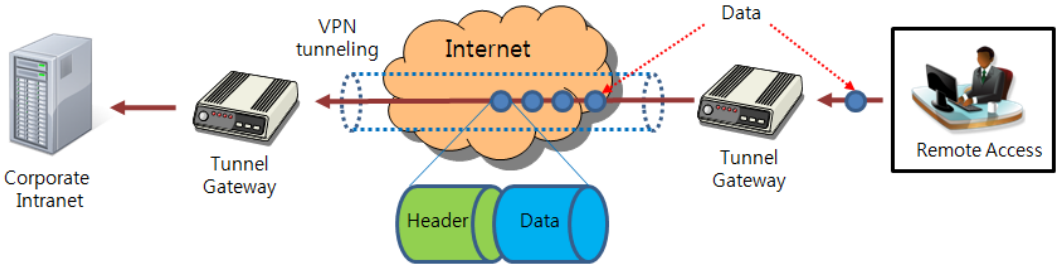


Figure 9. VPN Tunneling

3.2.3. IDS/IPS(Intrusion Detection/Protection System): This system is monitoring and intrusion analysis systems for all the packets transferred between computer systems and networks. The intrusion detection system detects the intrusion of unauthorized users so that system resources are effectively protected.

3.3. Storage Security

The main purpose of storage security is to protect sensitive information such as personal and enterprise information. In order to achieve this, it protects changes of the information by unauthorized users, information leakage, and destruction of information by the access control and data encryption. Since the access control for storage services grants the access permission by the users and blocks illegal access, it is possible to control a variety of access and monitor the specific session. Also, data encryption by each column is possible while only the authorized users can perform decryption. The storage security not only prevents illegal leakage due to data files and other physical methods, but also protects the sensitive information from an administrator who can access all data.

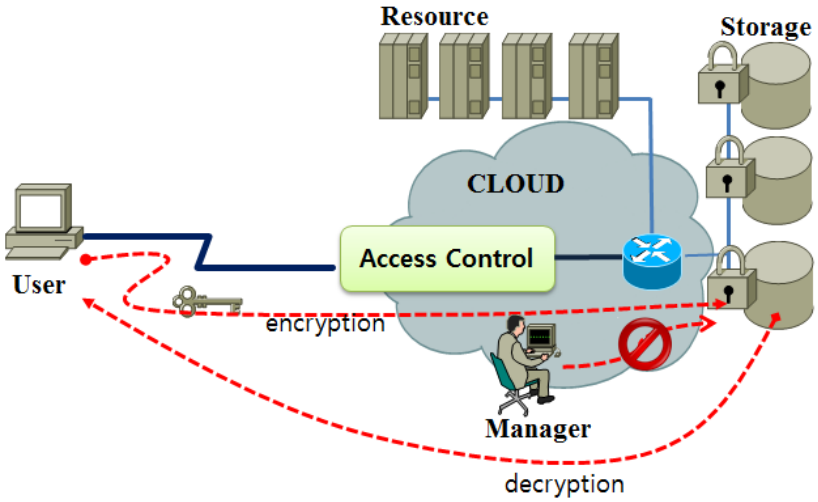


Figure 10. Data Encryption and Decryption for Stage Security

4. Requirements for Cloud Computing Security

With the development of the essential characteristics in cloud service, the security technology for information field of cloud computing has been also developed. However, it is not easy to prepare the security solutions that fully satisfy the security requirements. In order to have safe deployment of cloud services, we need to continuously update the standardization and the defense technologies for new threats. In this regard, CSA(Cloud Security Alliance) updates the elements for security management every year such that they define the cloud computing security requirements, which is able to cope with the new security threats as indicated in Table 1 [8].

Table 1. Cloud Security Requirements by CSA [8]

	Classification	Contents	Domain
V1.0(2009), Domain1~15	Cloud Architecture	Cloud Computer Architectural Framework	1
	Governing in the Cloud	Governance and Enterprise Risk Management	2
		Legal	3
		Electronic Discovery	4
		Compliance and Audit	5
		Information Lifecycle Management	6
		Portability and Interoperability	7
	Operation in then Cloud	Business Continuity and Disaster Recovery	8
		Data Center Operation	9
		Incident Response, Notification and Remediation	10
		Application Security	11
		Encryption and Key Management	12
		Identity and Access Management	13
		Storage	14
		Virtualization	15
V2.1(2010), Domain 1~13	Governing in the Cloud	Legal and Electronic Discovery (V1.0 Domain 3 + 4)	3
	Operation in then Cloud	Traditional Security, Business Continuity and Disaster Recovery (V1.0 Domain 8 + Traditional Security)	7
		Delete →Storage (V1.0 Domain 14, Delete)	-
V3.0(2011) Domain 1~14	Governing in the Cloud	Legal Issues : Contracts and Electronic Discovery (V2.1 Domain 3, Modify)	3
		Compliance and Audit Management (V2.1 Domain 4, Modify)	4
		Information Management and Data Security (V2.1 Domain 5, Modify)	5
	Operation in then Cloud	Incident Response (V2.1 Domain 9, Reduce)	9
		Identity, Entitlement, and Access Management (V2.1 Domain 12 + Entitlement)	12
		Security as a Service (New Content)	14

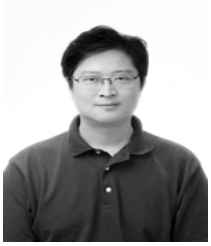
5. Conclusion

In recent IT environment, the biggest issues are virtualization, cloud services, and big data technology. Cloud services have many advantages such as the resource efficiency by virtualization, reusability, and energy efficiency such that many cloud services, *e.g.*, IaaS, PaaS, and SaaS are rapidly increased to provide the environment for saving and accessing documents and multimedia files. However, because the development of cloud services is based on the existing IT services, the problem has been pointed out that existing vulnerabilities and threats as well as virtualization and hypervisor vulnerabilities of information security problem exist. In this paper, in order to provide the view of security issues, we have been dealing with the issues of security threats and security technologies at the aspect of end users and providers. We also provided the security requirements for secured cloud computing services to cope with the new environment and additional security threats in cloud services.

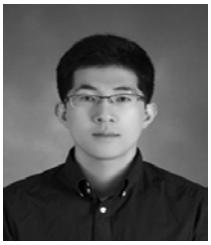
References

[1] I. Gul and M. Hussain, Distributed Cloud Intrusion Detection Model, International Journal of Advanced Science and Technology(IJAST), Vol. 34, pp.71-82**(2011)**
[2] A.q ur Rehman and M.Hussain, Efficient Cloud Data Confidentiality for DaaS, International Journal of Advanced Science and Technology(IJAST), Vol. 34, pp.1-10**(2011)**
[3] Shakeel Ahmad, Bashir Ahmad, Sheikh Muhammad Saqib and Rashid Muhammad Khattak, Trust Model: Cloud's Provider and Cloud's User, International Journal of Advanced Science and Technology(IJAST), Vol. 44, pp.69-80**(2012)**
[4] S. Lee, Security Considerations for Public Mobile Cloud Computing, International Journal of Advanced Science and Technology(IJAST), Vol. 44, pp.81-88**(2012)**
[5] G. S. Lee, D. G. Min and M. S. Jun, A Study on Authentication of Mobile Agency AP Connection Using Trusted Third Party in Smart Phone Environment, Journal of the Korea Academia-Industrial cooperation Society, Vol.13, No.11, **(2012)** http://dx.doi.org/10.5762/KAIS.2012.13.11.5496
[6] K. W. Lee and H. I. Jun, Mechanism of Multimedia Synchronization using Delay Jitter Time, Journal of the Korea Academia-Industrial cooperation Society, Vol.13, No.11, **(2012)**, http://dx.doi.org/10.5762/KAIS.2012.13.11.5512
[7] S. Y. Min and S. J. Jang, A Study on the Protection of Personal Information using a Virtual IDs in an Anonymous Bulletin Board, Journal of the Korea Academia-Industrial cooperation Society, Vol.13, No.9, **(2012)** http://dx.doi.org/10.5762/KAIS.2012.13.9.4214
[8] Y. S. Bae, A Study of Effect of In Information Security Management System Certification on Organization Performance, Journal of the Korea Academia-Industrial cooperation Society, Vol.13, No.9, **(2012)** http://dx.doi.org/10.5762/KAIS.2012.13.9.4224

Authors



Changsoo Lee received his B.S. degree in Computer Science from Hanseo University, Korea, in 1999, and M.S. and Ph.D. degrees in Computer Science from Soongsil University, Seoul, Korea, in 2002, and 2005, respectively. He is currently a researcher at network security lab in Soongsil University, Seoul, Korea. His research interests include multimedia applications and multimedia security, RFID/USN Solution.



Daewon Jung received his B.S. degree in Electronics and Communications engineering from Kwangwoon University, Seoul, Korea in 2006, and his M.S. and Ph.D. degrees in Information and Communications from Gwangju Institute of Science and Technology, Gwangju, Korea, in 2008 and 2012, respectively. He has been working for the Attached Institute of Electronics and Telecommunications Research Institute since 2012. His research interests include performance evaluation and protocol design for wireless communication systems and distributed protocols in wireless networks.

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.

