Analysis of Cloud Security Vulnerabilities and Countermeasures

Hyun-Min Son†, Nak-Keun Joo†, Hyun-Taek Choi††, Hyun-Cheol Lee††

Dongshin University†, DAISHIN Information&Communications Co., Ltd††

Summary
In recent years, cloud computing technologies have attracted attention as they provide efficient service any time and place based on such infrastructure resources as servers, storage and networks and such distributed processing technologies as virtualization. In a cloud computing environment in which all information is concentrated, service stability and security involving users and information resources will become core technologies. This study set out to predict security threats inside a data center by accumulating, processing and analyzing the diagnosis data of security vulnerability in public agencies and corporations and propose vulnerability items as objective grounds for the importance of security vulnerability and countermeasures against security threats, thus increasing the effects of checking and dealing with security vulnerability.

Key words:
Attack, Cloud Compyting, Security, Threats, Vulnerability.

1. Introduction

Cloud computing accumulates ICT resources such as storage, platforms and software as a shared pool at a data center, separates them as much as users need and provides service in virtualization technologies through a network. Security threats including new hacking and virus threats have emerged from the sharing of computing resources and led to the ongoing increase of adverse effects including the violation of information resources, cyber terrorism and the unauthorized release of personal and important information. They are now considered as serious social issues. In addition, cyber-attacks are increasingly more intelligent, advanced and automated including the advancement of malignant codes and attack techniques (e.g. Agent, Distributed, Automation and Stealth), rising cyber security threats between nations, and diversification of penetration pathways. The damage caused by electronic financial frauds is also on the rise based on malignant codes. A variety of techniques including phishing, pharming, smishing and memory hacking have increased consistently.
When a system is hacked, its outcomes appear in diverse phenomena. Once hacked, a system can be abused as a route to distribute malignant codes, path to leak corporate information or site of attack for other systems. Trying to solve these problems, public agencies and corporations have introduced and implemented a solution to diagnose and deal with the security vulnerability of IT infrastructure by the business area.
This study set out to check the security vulnerability of public agencies and corporations and propose their vulnerability items, thus securing a ground for priorities in responses to security vulnerability and suggesting a plan to build an efficient response system for security vulnerability to resolve security threats.

2. Related Researches

Cloud computing continues to change the ways of using and sharing data, applications, infrastructure and platforms, but many new security threats are emerging from clouds. In a general cloud environment, security threats can happen involving personal information, access authority, application and network security. Most virtualization platforms include device drivers, device emulators, and virtual machine management tools in addition to hypervisors, being exposed to security infringement more broadly than non-virtualization infrastructure. Different virtual machines share cash or bus, which means that a virtual machine can obtain data or encryption keys from another virtual machine sharing the same physical server. This raises the possibilities of security attacks. As a huge amount of data is stored in cloud service, it has naturally become a major target of attackers. There are ongoing technological research and development efforts to reinforce cloud security around the globe but there is no expecting the complete extinction of security threats.
In recent years, public agencies and corporations are redesigning the management process of vulnerability and establishing a vulnerability diagnosis and management system to deal with security threats more effectively in a cloud environment.
KT has, for instance, identified problems with the management of security vulnerability and established a web-based system for the diagnosis and integrated management of vulnerability and a process for its operation[1]. Hankuk Aviation University has proposed a quantitative assessment system to calculate the importance of security vulnerability in domestic software in a quantitative manner[2]. Hanyang University has proposed a security policy capable of security vulnerability analysis, prediction of attacks and rapid responses in case of DoS

Manuscript received February 5, 2019
Manuscript revised February 20, 2019

attacks based on TCP/IP[3]. Soonchunhyang University has analyzed the security policy and vulnerability in the surveillance and control system of national infra-structure[4]. The Board of Audit and Inspection has figured out the principles applied to the security control of information systems and proposed plans for checking the security control vulnerability applicable to the inspection of information systems in the public sector, presenting them as security control and inspection modules for the information systems of agencies in their regular audit and inspection sessions[5].
In addition, the Ministry of Science and ICT and the Korea Internet & Security Agency have published a detailed set of guidelines to analyze and evaluate technical vulnerability and presented a bunch of methods to check technical vulnerability by the analysis and evaluation item, thus allowing for the analysis and evaluation of various vulnerabilities[6].

3. Analysis of Cloud Security Vulnerabilities

3.1 Security Vulnerabilities and Analysis Tools

Security vulnerabilities refer to vulnerabilities with security found in software and information systems. They include threats to allow illegal user access to an information system, hinder normal service in the system, and leak, alter or delete important data managed in the system[7,8]. In general, attackers identify security vulnerabilities in a system, attack them and obtain the authority to control the system. They further abuse the system to distribute malignant codes or attack another system. Security vulnerabilities are classified into system, network, and application program security vulnerabilities.
• System security vulnerabilities: These are found in accounts, authority, file management and service related to a system and include race conditions, environment variables, accounts and passwords, access authority, system configuration, network configuration, buffer overflow and backdoors.
• Network security vulnerabilities: These concern network equipments, devices and structures and include unnece-ssary service and information provision, DoS, RPC, HTTP, SMTP, FTP, BIND, FINGER and buffer overflow.
• Application program vulnerabilities: These concern vulnerabilities in web browsers and servers, firewall servers, IDS servers, database servers and source codes.

There are automation tools that check whether there are security vulnerabilities in an information system, analyze the security level of the system based on the results, and offer assistance to the check and analysis of security vulnerabilities. These tools are called "Analysis tools for Security Vulnerabilities". There are a wide range of tools to analyze and check security vulnerabilities including the followings:
• Tools to check vulnerabilities: SATAN, SAINT, COPS, K-COPS, Nessus, nMAP, Snort, TCP-Wrapper, IPChain /IPTable, Antisniff, TIGER, ISS.
• Tools to detect and attack vulnerabilities: mSCAN, SSCAN, Nikto, X-Scan and N-Stealth.
• Tools to detect alteration in log files: Check Log and Chkwtmp.
• Port scanning: Port Sentry, Scan Logd, and Scandetd.
• Scanning attacks: Nmap, FPing, SING, HPWG, and PortQry.
• Tools to check file integrity: Tripwire, FCheck, AIDE, and MD5.
• Tools to perform and analyze logging: Swatch and ClearLog.
In the checking and analysis of vulnerabilities, they usually identify a set of check items to threaten the stable operation of an information system and also a set of detailed check items. Then an organic evaluation follows involving the vulnerability grade and improvement direction for the identified vulnerabilities.
The vulnerability check and analysis items are categorized into managerial, technological and physical fields:
• Managerial field: This field covers vulnerabilities with management, information protection and management and human resource management.
• Technological field: This field covers vulnerabilities with computer/communication, information protection systems, and system development.
• Physical/environmental field: This field covers physical and environmental vulnerabilities.

The present study divided the diagnosis areas into Unix, Windows, WEB, WAS and DBMS to check security vulnerabilities and the vulnerability groups into 15 items by the diagnosis area. Table 1. shows the categories of related checks and the number of items.

Table 1: Vulnerability groups and the number of check items

Category	UNIX	WIN	WEB	WAS	DBMS
Authority management	-	-	-	-	8
Setting	-	-	18	5	-
Log management	2	5	-	-	-
Patch management	6	3	-	-	-
Security patches	-	-	2	1	1
DB management	-	1	-	-	-
Check of environment files	-	-	-	-	6
DBMS security setting	-	-	-	-	15
Solution vulnerabilities	-	-	8	1	-
Security management	-	20	-	-	-
File and directory management	20	-	-	-	-
Account management	15	18	-	-	-
Service management	35	35	-	-	-
Security audit setting	-	-	-	-	2
Access control	-	-	-	5	-

3.2 Integrated Check of Security Vulnerabilities in a Cloud Environment

There are two types of methods to diagnose vulnerabilities: manual and automatic diagnosis. Automatic diagnosis methods use scripts supported by the server to diagnose vulnerabilities automatically.
The present study checked security vulnerabilities by the area based on the check items of vulnerability groups by using an automatic tool to check vulnerabilities called "Secuguard SSE". The overall system diagram is found in Fig.1.

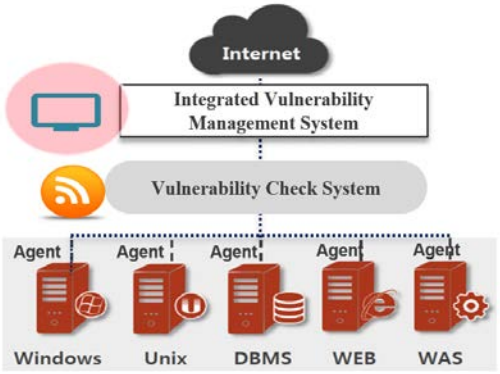

Fig. 1 System to check security vulnerabilities

In the process of checking security vulnerabilities, agents installed at each server and system collect data. Then, the data is analyzed/diagnosed in the system designed to check vulnerabilities.
Users can retrieve/analyze vulnerability diagnosis results in the integrated system for vulnerability management. Fig.2 shows the overall process of checking security vulnerabilities.

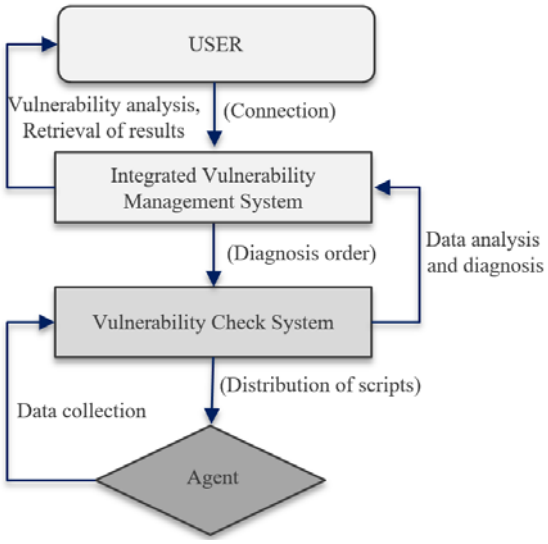

Fig. 2 Process to check security vulnerabilities

3.3 Analysis of Cloud Security Vulnerabilities

Table 2. shows the diagnosis results of security vulnerabilities by the diagnosis area, diagnosis number, total number of items and good ratio(%).

Table 2: Diagnosis results by the area

Diagnosis Area	Diagnosis Number	Total Number of Items	Good	Vulnerable	Good Ratio (%)
UNIX	532	41,496	40,661	835	97.99
WIN	114	9,348	9,111	237	97.46
WEB	89	2,492	2,448	44	98.23
WAS	122	1,464	1,385	79	94.60
DBMS	90	3,690	3,416	274	92.57
Total Number	947	58,490	57,021	1,469	97.49

Table 3. shows the analysis results by the vulnerability group. Vulnerable groups to security threats were found in DBMS security setting, account management, security management, security inspection setting, security patch, patch management, access control, setting, service management, and file and directory management.
The most vulnerable groups were access control(74.72%), DB management(87.51%) and security patch(89.56%).

Table 3: Good ratio by the vulnerability group(unit: %)

Vulnerability Groups	2018			2019	Average
	Q2	Q3	Q4	Q1	
Authority management	94.08	92.93	97.33	97.36	95.43
Setting	78.10	90.28	97.86	97.65	90.97
Log management	73.37	99.66	99.82	99.88	93.18
Patch management	82.95	95.40	96.10	96.49	92.74
Security patches	89.74	88.81	89.93	89.74	89.56
DB management	80.24	88.71	90.73	90.35	87.51
Check of environment files	93.20	97.31	98.19	98.15	96.71
DBMS security setting	93.34	93.92	93.89	93.78	93.73
Solution vulnerabilities	95.75	98.73	99.68	99.60	98.44
Security management	95.60	97.55	98.43	98.46	97.51
File and directory management	81.72	94.00	94.21	94.04	90.99
Account management	77.63	97.63	98.48	98.36	93.03
Service management	96.58	98.90	99.11	99.12	98.43
Security audit setting	97.02	90.91	90.76	89.44	92.03
Access control	39.20	76.28	92.40	90.98	74.72

The vulnerability analysis results show the vulnerability items(diagnosis area and good ratio) under the average by the vulnerability group as follows: the most vulnerable items were "Vaccine Program Update" under patch management, "/etc/hosts file owner and authority setting" under file and directory management, and "DBLINK encryption setting" under DBMS security setting in the order.

• DBMS security setting: DBLINK encryption setting (DBMS, 55.56%), limited use of registry extended stored procedures(DBMS, 84.44%), designation of connection IP(DBMS, 86.67%), and use of PL/SQL Package(DBMS, 87.78%).

• Account management: regular password change(DBMS, 54.44%), password complexity setting(DBMS, 72.22%), cataloging of accounts(DBMS, 76.67%), and unlimited log-in block setting(DBMS, 81.11%).

• Security management: LAN manager authorization level (WIN, 80.7%).

• Security inspection setting: DB inspection performance setting(DBMS, 87.78%).

• Security patch: the application of the latest patches (DBMS, 65.56%).

• Patch management: vaccine program update(WIN, 5.61%) and the application of the latest HOT FIX(WIN, 72.81%).

• Access control: manager password management(WAS, 83.61%), manager console management(WAS, 87.70%), and change of the manager's account name(WAS, 88.52%).

• Setting: response message management(WEB, 68.54%).

• Service management: inactivation of NFS service(UNIX, 87.41%) and block of HTTP/FTP/SMTP banners(WIN, 84.21%).

• File and directory management: /etc/hosts file owner and authority setting(UNIX, 6.95%) and check of World Writable files(UNIX, 87.78%).

3.4 Security Measures for Vulnerability Items

Security vulnerabilities exist as defects until a security patch is provided by application, OS and equipment manufacturers. Attackers use a range of attack techniques to find invisible defects. It is thus critical to protect information resources from such diverse attempts by eliminating security vulnerabilities and keeping information resources safe from security threats. The following security measures and responses can be used to resolve vulnerability items under the average:

• DBMS security setting(DBMS)

When there is no encryption of DBLINK between a client and database, important information such as passwords can be exposed in access to a distant server. It is thus important to ensure DBLINK encryption between a client and database. Registry extended stored procedures can read or update important information in the Window registry and should thus be limited in their use.

Important data and DB access should be limited to allow for access only for trusted IP. The concerned PL/SQL package should be controlled not to grant "Execute" authority unnecessarily to "Public".

• Account management(UNIX, WIN and DBMS)

After reviewing the influence of service, the manager should limit, delete or lock unnecessary accounts not in practical use such as unauthorized accounts, retirees' accounts and test accounts. Prohibition of passwords that can be inferred easily, complexity setting(mixed use of characters, numbers, and special characters; there should be nine or more) and regular change of passwords(every 90 days). If the system is set to allow for infinite log-in attempts, there is a risk that attackers can obtain a log-in account through "Brute Force Aattacks". The number of failed log-in attempts should be limited by the setting of threshold value for account lock. In such a case, an account should be locked for 30 minutes or longer. Console access should be authorized only for the user accounts that need it and limited for the distant terminal groups and accounts. The authority of user access and termination should be controlled by the grade.

• Security management and inspection setting(WEB, WAS and DBMS)

The use of major information in the Window registry should be limited. It should be set to automatic log-off or lock when the user does not use for a certain amount of time. There is a need to set a screen saver, limit the waiting time under ten minutes and use a code to clear the screen saver.

• Security patch and patch management(UNIX, WIN, WEB, WAS and DBMS)

The installation of vaccine programs itself is not enough due to the continuous emergence of new viruses. A function is needed to update virus information regularly and treat even the latest viruses. HOT FIX is a program distributed to patch for major vulnerabilities that should be corrected. It is recommended that the program should be installed as soon as possible after its release. Vulnerabilities should be removed by the regular application of the latest patch for each version.

• Access control(WAS)

The manager's account should use a password that is encrypted or difficult to infer. It manages all the authority related to WEB. When it is used not via the manager console, access to it should be impossible via the default port. It sets the authority for password files.

• Setting(WEB, WAS)

There is a need to manage authority for log files since they can contain useful information for attackers. When it is linked to other applications for logging directory and file management and thus needs access authority for the account of "Application Linkage," it can have impacts on service. There is a need to review the impacts. The header information of response messages should be hidden as attackers can leak the header information of the web server intentionally to obtain the information of the target system. The web server daemon should be managed not to be used by the root authority.

• Service management(UNIX and WIN)

The NFS(Network File System) service has a high risk of infringement accidents to allow for the root authority and should thus be suspended when not in use(inactivation of the daemon related to the NFS service). There is a need to eliminate the basic items to be shared or limit access to the system resources. It is needed to control the NetBIOS access and limit the use of FTP service.

• File and directory management(UNIX)

There is a need to control access authority for "/etc/hosts files" used in the mapping of IP addresses and host names. When there is a file set by the authority for all users to access and revise, general users' mistakes or malicious behavior can cause the leak of major file information or system failure. It should thus be limited(checking the words writable files). General users should not be allowed to revise the home directory that can be revised only by its account.

4. Countermeasures against Cloud Security Threats

4.1 Cloud Security Threats

There is a concentration of important information in the shared cloud pool in a cloud computing environment, which is why attackers target it. Attackers can also expand the scope of attack easily and are highly likely to hack the cloud through various attacks and advanced techniques. In the cloud environment, users can share files with one another. When a user uploads a file infected with a malignant virus on the cloud server, it can cause broader damage. The analysis results of security vulnerabilities identified good examples of cloud security threats as follows:

• System vulnerabilities: These are bugs in programs, systems, and OS. Attackers invade a system, leak information, take the system control authority or stop the service operation via this medium. The OS vulnerabilities can, in particular, expose all the service and data security to huge risks.

• Certification information and access authority management: Insufficient ID, certification information or key management allows for unauthorized access to data and can cause serious damage to the agency or end user.

• UI and API design: There is a risk of exposure in software user interface(UI) or API used to manage and manipulate cloud services including provisioning, management and monitoring, which raises a need to design UI and API to prevent malicious attempts to detour the security policy.

• Account management: Once obtaining the certification information of a user, attackers can manipulate data, return forged information and manipulate a client with an illegal site. They can also damage the confidentiality, integrity and availability of the concerned service with the stolen certification information.

• Vulnerabilities of cloud sharing: Cloud service shares information, infrastructure, platforms or applications and thus provides service expandability, but it has the vulnerabilities of sharing technology that can be abused. The damage caused by the security vulnerabilities of clouds can be even bigger by the damage caused by the old systems, which raises a need to provide smart-combined preventive measures that have further evolved from the current ones on an ongoing basis. It is also needed to prepare reinforcement plans to minimize damage in case of security accidents despite these preventive measures. There should be powerful security policies for newly evolving security threats including technological countermeasures to apply and combine various security technologies and emerging technologies, expansion of

insurance and reward systems, distribution of insiders' access authority, security education and strict punishment regulations for accidents caused by the inattention of service providers.

4.2 Plans for Basic System Configuration to Improve Security Vulnerabilities

A response system for security vulnerabilities can be organized by providing transparent information about the security technologies, processes and systems of clouds, figuring out the security abilities in details, and reacting to security threats with reinforced security policies. Public agencies and corporations need to build a reinforced access authority management system, ensure the encryption of important data, and apply security standards including HTTPS, TLS, SSL, IPSec and SFTP to reinforce the data security of networks to connect users to clouds. In addition, they have to find causes of security violation, reduce recovery time, and minimize data losses.

A basic system safe from security vulnerabilities and threats should separate WEB from WAS under the same system, build three layers of WEB, WAS and DBMS and ensure dualization for reliability. Fig.3 shows a block diagram of three layers including WEB, WAS and DBMS.

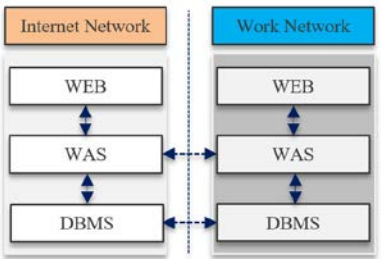

Fig. 3 Organization of WEB, WAS and DBMS

When a work network is linked to the Internet network, the information system network should be separated to minimize connection points and ensure efficient security management. Only necessary data should be transmitted between the work and Internet network via the data transmission system. It is also needed to build data-linked infrastructure based on storage between a physically or logically block work network and the Internet network and run a stable data transmission system by establishing a system with separate work and Internet networks and synchronizing only altered data.

In use of sharing storage(NAS), real-time log creation should be prohibited with its use only as an attached file. Service management for distributed files(WAR, JSP, Class and so on) should be sublated. When WAR(Web Application Archive) files are piled upon NAS, all the load may be concentrated on NAS and thus lower its performance. When there is a disorder in NAS, it can cause a disorder to the entire work system. It is thus required to provide service at the individual VM level and allow only for simple errors in NAS so that reliable service can be maintained.

4.3 Application Development based on Security Threats

In principle, IP, host names, and domain hard coding should be prohibited within an AP source in the development process. In case of logs in large numbers, the deterioration of performance will make it impossible to analyze the logs, which raises a need for WAS log management. It should be set to control logs of the same repeating content and leave no SQL query in logs. In case of connection to many databases, even user log-in itself can cause massive load. The main page should minimize its load and produce and provide entire or partial files in batch at certain time intervals. In case of connection to other systems, the link information should be provided in a non-synchronized manner rather than real time.

Static contents(HTML, images, documents and videos) should be separated into the WEB server. WAS should prohibit the service of video files and use the video server for the service. The use of session clusters should be reduced to the minimum since it can impose load on the synchronization of the entire node sessions within WAS and cause a system disorder after OOME(Out of Memory Error) in the use of session clusters.

4.4 Use of Open Software

It is important to react to security threats by continuing to remove security vulnerabilities and maintain ongoing quality control and risk management activities until the elimination of security vulnerabilities. Applications, OS and equipments launched by a reliable vendor have fewer defects and vulnerabilities with the products and can activate a security process fast. It is also important to use products from a vendor that keeps quality control consistently, use a vaccine program and apply the latest updates and security patches rapidly.

After a copyright holder makes the source codes of open software public, one should use open software that anyone can use, replicate, distribute and revise in a free and unlimited manner to share and manage the latest technological information, problems and solutions freely and enable fast and flexible development. Open software uses open formats or protocols, thus ensuring mutual linkage between different software products. Since outstanding developers take direct part in development, it ensures relatively stable operation compared with independent

programs. Since the source codes are made public, anyone can detect security vulnerabilities easily and correct bugs. When sources are made public, however, they can cause security threats, which raises a need to take ongoing interest in security threats and make efforts to solve problems.

5. Conclusion

Cloud is a service to borrow IT resources including computing, storage, software, and networks via the Internet as much as one needs and pay for the amount of service that one uses. In cloud computing where all information is concentrated, the major systems become the targets of hacking attacks, whose techniques are increasingly more advanced and intelligent. Cloud computing has many advantages including low costs to process information and provide high performance, reduced time to build and develop a system, and flexible expansion. There are, however, various security threats in it.

The present study analyzed security threat elements inside a data center and provided objective data about the vulnerability groups and items as to the importance of security vulnerability. It also proposed a set of plans to reinforce security by identifying problems with information threats, analyzing security vulnerabilities, and making a plan to deal with them. Future research directions include the development of a tool to check and analyze security vulnerabilities in intelligent clouds to check the security vulnerabilities of a system automatically and provide solutions for the identified vulnerabilities and problems.

References

[1] Ho-Geon Mun and Seong-Cheol Park, "A Integrated Management System to Diagnose Vulnerabilities for Reinforced Corporate Security," Korean Journal of Communications and Networks, Issue 31, Vol. 5, April 2014, PP.39~45.
[2] Jun-Seon Ahn, et al. "A Study on a Quantitative Evaluation System for the Importance of Security Vulnerabilities," Journal of The Korea Institute of Information Security and Cryptology, Issue 25, Vol. 4, August, 2015, PP.921~932.
[3] Seong-Hyeon Jo, et al., "Analysis of DoS Attack Vulnerabilities and DoS Attack Cases in TCP/IP Network Protocols," Journal of The Korea Institute of Information Security and Cryptology, Issue 24, Vol. 1, February, 2014, PP. 45~52.
[4] Myeong-Gyun Choi, et al., "Analysis of Security Policy Trends and Security Vulnerabilities in Control Systems," Journal of The Korea Institute of Information Security and Cryptology, Issue 21, Vol. 5, August, 2011, PP.55~64.
[5] Yeong-Ho Baek, "A Study on Plans to Check the Security Control Vulnerability of Information Systems in the Public Sector," Audit Research Institute at the Board of Audit and Inspection, April, 2015.
[6] Korea Internet & Security Agency and Ministry of Science and ICT, "Analysis of Technological Vulnerabilities and Detailed Guidelines for Evaluation Methods," December, 2017.
[7] http://www.nilesoft.co.kr
[8] http://www.itworld.co.kr/

Hyun-Min Son received M.S. degree in computer Science for Dongshin University, Korea. He works for DAISHIN Information& Communication Co, Ltd. His research interest include Security, Cloud Computing and SI Construction.

Nak-Keun Joo received Ph.D degree in computer Science for Chonnam University, Korea. He teaches digital contents protection as an full professor at Dongshin University. His research interest include Computer Algorithm, Security, Cloud Computing and Digital Watermarking.

Hyun-Taek Choi received master degree in the Department of Business Administration for Hongik University, Korea. He works for DAISHIN Information & Communication Co, Ltd. His research interests include Management Information, IT Marketing and Public SW.

Hyun-Cheol Lee received Ph.D degree in Computer Science for Dongshin University, Korea. He works for DAISHIN Information& Communication Co, Ltd. His research interest include Security, Cloud Computing, Network Protocol, AR/VR and Realistic Media.