Two Factor Authentication for Cloud Computing

Shirly Lee, Ivy Ong, HyoTaek Lim and HoonJae Lee, *Member, KIMICS*

***Abstract*— The fast-emerging of cloud computing technology today has sufficiently benefited its wide range of users from individuals to large organizations. It carries an attractive characteristic by renting myriad virtual storages, computing resources and platform for users to manipulate their data or utilize the processing resources conveniently over Internet without the need to know the exact underlying infrastructure which is resided remotely at cloud servers. However due to the loss of direct control over the systems/applications, users are concerned about the risks of cloud services if it is truly secured. In the literature, there are cases where attackers masquerade as cloud users, illegally access to their accounts, by stealing the static login password or breaking the poor authentication gate. In this paper, we propose a two-factor authentication framework to enforce cloud services' authentication process, which are Public Key Infrastructure (PKI) authentication and mobile out-of-band (OOB) authentication. We discuss the framework's security analysis in later session and conclude that it is robust to phishing and replay attacks, prohibiting fraud users from accessing to the cloud services.**

***Index Terms*— Cloud Computing, Mobile OOB Authentication, PKI Authentication, Stream Cipher, Two-Factor Authentication**

I. INTRODUCTION

IN today's high technology era, Internet is not longer only a communication medium but due to its reliable and ubiquitous broadband access, it is now transformed to a

powerful computing platform. Instead of running applications software and managing data on centralized or in-house infrastructure, now we are able to run the applications and access data on demand from "cloud" anywhere anytime. The high demands of computing resources have prompted organizations to outsource their storages and computing needs [1]. Cloud computing might be one of their choices as cloud computing is the Internet computing paradigm which provides unlimited infrastructure to store and execute data or applications.

Although cloud computing able to help organizations accomplish more by breaking the physical bound between IT infrastructure and its users. However most of users cannot afford the risk to compromise the security of their applications and data [2]. For example, International Data Corporation (IDC) conducted a survey from 264 IT executives/CIOs and their line of business (LOB) colleagues in Q3 year 2009 to study the issues and concern of their companies' used cloud computing. From the result as shown in Fig. 1, security again ranked first as the greatest challenge or issue in cloud computing [3]. This is mainly due to customers lose control over physical security in cloud model; they are sharing computing resources with others companies so security concerns such as how to safeguard data/application from unauthorized access, use, disclosure, disruption, modification or destruction always arise when both customer data and program are residing at the provider premises.

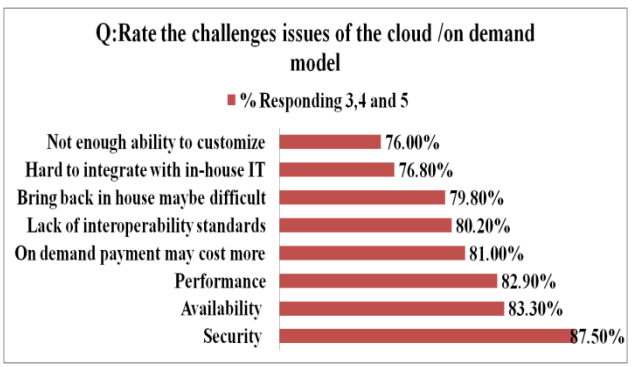

Fig. 1. Result of IDC Q3 Year 2009 Survey

Beside this, identity theft is one of the prevalent issues in cloud environment too. Studies indicate that digital identity fraud is still on the rise with an increase in sophistication and the expansion of attack vectors. One of the most exploited methods today is the gaining of account access by stealing reusable credentials for web sites that yet to implemented "strong" user authentication.

Manuscript received July 7, 2010; revised July 13, 2010; accepted July 21, 2010.

Shirly Lee is with the Department of General, Dongseo University, Busan, Korea (Email: shirlyl.lee@gmail.com)

Ivy Ong is with the Department of General, Dongseo University, Busan, Korea (Email: ivy_ong2000@yahoo.com)

Hyo Taek Lim is with the Department of Computer & Information Engineering, Dongseo University, Busan, Korea (Email: htlim@dongseo.ac.kr)

Hoon Jae Lee, Corresponding Author, is with the Department of Computer & Information Engineering, Dongseo University, Busan, Korea (Email: hjlee@dongseo.ac.kr)

Further to this, most common implemented authentication methods are knowledge-based, which user ID and password are requested only once during login. This ID password method provides higher level of convenience to users but also requires less effort for attackers to exploit. Many attacks are manifested as "phishing" messages that masquerade as the one that sent by legitimate organizations and contain URLs that point to fraudulent web sites which have the same appearances as genuine ones [4]. The incident of Salesforce.com, customers hit with phishing attack in year 2007 [5] is the good example to show that user ID and password authentication method is not strong enough to against the access security attack in clouds.

In this paper, we propose a two-factor authentication framework in cloud computing via two different communication channels: using *PKI Web based authentication* and mobile phone based *OOB authentication.* A random one-time authentication code based on *NLM-128 generator* has been including in this framework to ensure the randomness of the authentication code, so that attackers will not able to guess the next authentication code in sequences. The rest of the paper is organized as follows. Section II outlines the related research works. Section III describes our two-factor authentication framework. We carry out a security analysis of our proposed authentication framework in Section IV and conclude the paper in last Section V.

II. RELATED WORK

A. Cloud Computing and its Security Threats

Cloud computing is a paradigm that incorporates the ideas of software, platform, infrastructure and computing resources as Internet-based services. Users neither own the physical location nor know if other sources of data collectively stored with theirs. The term "cloud" is introduced since 1990s when Virtual Private Network (VPN) services are used for data communication [6]. Similar to VPN concept, cloud computing establishes a virtual computing environment that is dynamically allocated to users on demand. The main providers in this field include Google, Microsoft, Amazon, Yahoo, IBM, HP and Intel [7]. Google Apps, Amazon Simple Storage Service (Amazon S3), Amazon Web Services (AWS) and Amazon Elastic Compute Cloud (EC2) are some popular examples of cloud services.

Despite the advantages it brings, cloud computing is exposed to many security threats due to its unique architecture and characteristics. The massive concentration of resources and data become a new base for attackers. A broad set of policies, technologies and controls with different complexities should be deployed to protect the interfaces, transmission mediums, data and infrastructures of different cloud service models: *Software as a service (SaaS), Platform as a service (PaaS) and Infrastructure as a service (IaaS).* Cloud Security Alliance (CSA) is a non-profit organization that formed to aid both users and providers by providing best practices for cloud computing security. Recently CSA has identified and published the "top threats to cloud computing" report in [8]. Among all, we focus on the study of insecure cloud interfaces/APIs where strong authentication and access control are required in concern with secure encrypted transmission. In addition to alleviate the threat of service hijacking where credentials/passwords are often reused in practices, a possible remediation is to embed with a robust two-factor authentication function.

B. Two- Factor Authentication

Authentication play a very important role to ensure only authorized user allow to access the application by verify the user identity before any accesses grant to the user for the underlying services. Two-factor authentication is a combination of two authentication methods to increase the assurance that a correct user has been authorized to access a secure system or server. The Two factor authentications make it more difficult for unauthorized user to access or use the application .In this paper, we achieve the objective by adding a mobile OOB authentication on top of a PKI authentication process during the cloud user login phase.

C. Public Key Infrastructure (PKI) Authentication

PKI is a combination of software, hardware, policies, procedures and people that work together to provide a high level of security functions on network, especially useful in e-commerce businesses and online banking transactions. It meets the basic security goals of confidentiality, integrity, secure authentication and non-repudiation. A PKI authentication environment can be constructed through the public key certificates and digital signatures from a Trusted Third Party (TTP) – Certificate Authority (CA) approach. The traditional authentication method with user ID and password is cost-effective, yet it poses a very low level of security and is susceptible to attack. In PKI authentication scheme, CA issues the user a secure digital certificate "ID", where the authority information such as identities, credentials or affiliations is bound with his/her public key and safely sealed with a digital signature using the CA's own key for a given period of time. In such a way, trust in the user key relies on one's trust in the CA's key validity.

Suguru and et al. develop an Opengate-PKI [9] certificate-based authentication gateway to authenticate network users as well as to record the usage logs. Users submit their certificates issued by CA to the Opengate-PKI through web browser. Opengate-PKI converts the SSL handshake packets in HTTPS form into EAP-TLS form, and authenticates it with a RADIUS server. User may access to the network if the authentication process succeed, else Opengate-PKI will change the certificate-based authentication method to ID/Password-based approach. Another interesting lightweight PKI (LPKI) [10] has been introduced by Mohsen and et al., to effectively decrease

the computational costs and communication overheads for mobile devices in resources limited platform. LPKI deploys Elliptic Curve Cryptography (ECC) in contrast to the conventional PKI such as PKIX and WPKI that use modular exponentiation (RSA). Moreover, it adopts signcryption technique which is opposed to the well-tried signature-then-encryption scheme that faces low efficiency and high cost of summation problems. LPKI assigns only one pair of private-public keys to each subscriber and delegates all validations to a Validation Authority (VA).

D. Out- Of-Band (OOB) Channel

OOB channel is a technique used for transferring secret information, such as a one-time password to another trusted party using a different communication channel outside a previously established channel. Rather than relying on a single possibly attackable channel, it is viewed as a mean to prevent security frauds by separating sensitive data or credentials being delivered to another channel. OOB authentication service may leverage users' mobile phone as the second factor of authentication to improve the strength of authentication, particularly the resilience to common phishing attacks. Many online banking services are adopting OOB type of protection, which verifies users' identities through a separate channel to against those real-time threats.

E. Random Number Generator (RNG)

Instead of using a vulnerable and seldom-updated static password, an alternative way is to use RNG to produce a sequence of numbers or symbols that are random and unpredictable. Basically RNG can be categorized into: *Pseudo-random (PRNG)* or *True-random (TRNG)* [11]. TRNG is more costly and normally built on top of hardware while PRNG is easier to be implemented in software using cryptographic primitives like a block cipher running on counter mode. In our framework, we use NLM-128 generator to generate a keystream as the one-time session code. This output keystream is only valid for a single login session and is random; prevent to be predicted for future keystreams.

F. NLM-128 Generator

NLM-128 is an enhanced LM-type summation generator [12], added with a de Bruijn-type [13] [14] Nonlinear Feedback Shift Register (NFSR) to improve the nonlinearity and unpredictability of the output keystream. The existing Linear Feedback Shift Register (LFSR) of length 127 bits and the new NFSR of length 129 bits give the NLM-128 an internal state of 258 bits. It takes a 128-key, *k* and a 128-bit initialization vector, *iv* to fill the internal state.Fig. 2 shows the XORing of LFSR, a_j and NFSR, b_j sequences together with carry, c_{j-1} and memory, d_{j-1} sequences at time *j* yields the output keystream, z_j.

$$z_j = y_j \oplus d_{j-1} = (a_j \oplus b_j \oplus c_{j-1}) \oplus d_{j-1} \quad (1)$$

$$c_j = f_c = a_j b_j \oplus (a_j \oplus b_j)\, c_{j-1} \quad (2)$$

$$d_j = f(a_j, b_j, d_{j-1}) = b_j \oplus (a_j \oplus b_j)\, d_{j-1} \quad (3)$$

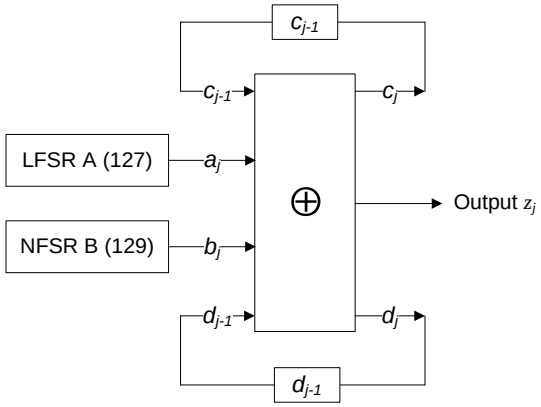

Fig.2. NLM-128 Generator

The empirical result concludes that NLM-128 is able to defeat the known attacks against typical and LM-type summation generators, such as divide and conquer attack and fast correlation attack.

III. PROPOSED FRAMEWORK

A. PKI Authentication

Firstly, user has to prove his/her identify to the cloud web server by using his/her PKI and user password.

B. One-Time Authentication Code

After validated the user password and PKI, web server will send an authentication request to the cloud authentication server. The authentication request consists of user ID, password and timestamp. Upon receives the request, authentication server will decrypt the request message and send user password and timestamp to NLM-128 generator to generate a one-time authentication code. This code is only valid for a single login session and it is random, so that attacker does not able to predict the next sequence code. The authentication code will be forwarded to the web server and user's workstation. At the same time, the same code will be SMS to the user's mobile phone. This SMS contains link that will direct user's mobile build in WAP/GPRS browser to contact the dynamic generated page from the cloud web server. This page presents user with a choice to allow or deny the session.

C. Out-Of-Band (OOB) Channel

User compares and verifies the displayed authentication codes from his mobile and the workstation. If the authentication codes match, user chooses "accept" to allow the session. If user accepts the connection, web server checks if the code matches the one it just received and decrypted from the authentication server. If matches, it will setup a secure connection and grants access to the user; otherwise an error message is sent to the user indicated denied access. The secure connection could be achieved using SSL, IPSec or VPN. If user chooses to disallow the session, user is asked if fraud has been taken

place. Fraud might happen if attacker stole the user's PKI. In this case, user can select an option on mobile phone to lock his/her account until further notice.

Our proposed authentication framework is illustrated in Fig. 3, which has eight steps:

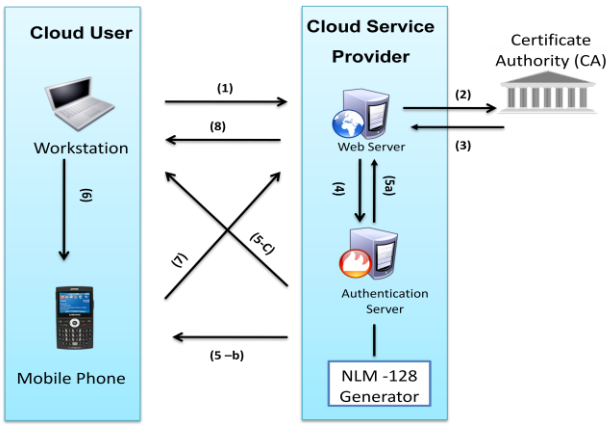

Fig. 3. Two-Factor Authentication Framework

(1) User has to prove his/her identify to the cloud web server using his/her PKI and user password.
(2) Web server sends the PKI to CA for user identity verification.
(3) CA replies the verification result.
(4) After validated the user password and PKI, web server sends an authentication request to the authentication server. Otherwise an error message is sent to the user rejecting his/her access and this terminates the authentication process. The authentication request consists of user ID, password and timestamp. Upon receives the request, authentication server will decrypt the message and use NLM-128 generator to generate a one-time authentication code.
(5-a) The authentication code will be sent to the web server.
(5-b) At the same time, the same code will be SMS (consists of WAP/GPRS link that will contact authentication server dynamic page which allows user to decide whether to accept or deny the connection) to the user's mobile phone.
(5-c) The same code will also be forwarded to the user's workstation and displayed as session name.
(6) User compares and verifies the displayed authentication code from his mobile and the session name from the workstation.
(7) If the authentication codes match, user chooses "accept" to allow the session.
(8) If user accepts the connection, web server checks if the code matches the one it just received and decrypted from the authentication server. If matches, it will setup a secure connection and grants access to the user. The secure connection could be achieved using SSL, IPSec or VPN.

The above described authentication steps need to be done within a given timeframe. This is to assure the access credentials are only to be used within the given timeframe. Lastly user may terminate the session by either closing the browser from the workstation or by revisiting the approval page on the mobile or disallowing the session. The option of allow user to terminate the session from mobile phone is useful for the case when user away from the workstation and forgot to log out. However web server will also expire the user's session after certain idle time.

IV. SECURITY ANALYSIS

This chapter contains the security evaluation of our proposed framework. The security features are presented as below.

A. Identity Proofing Protection

Our proposed framework addresses identity proofing with two-factor authentication: PKI authentication and mobile OOB authentication. Security of the system depends on the security of messages sent by SMS and WAP/GPRS. Only user's registered mobile phone can receive the short message containing one-time authentication code and obtain the proper WAP/GPRS page from authentication server. Only the mobile phone can acknowledge the choices on the page. When the web server receives "accept" with the authentication code, it knows that is indeed initiated and approved by user. Further to this, authentication code is not possible to guess since it appears as a random number.

B. Defense Replay Attack

Each authentication code is used exactly once. Once it is sent and verified, it is no longer valid for reuse. Further to this, timestamp has been used to defense replay attack, the access credential are only valid to be used within the given timeframe.

C. Hijacking Attack Protection

An attacker might try to hijacking the session to get unauthorized access, however our proposed framework able to countermeasure this as it requires user to acknowledge via the SMS with a one-time authentication code before given any access right to the user. Once user pass the OOB authentication, a secure connection will then be established, so user will be able to transfer or access to the clouds without worry.

D. Forward and Backward Secrecy

Since the next authentication code is randomly generated and unpredictable, there is no risk for any used authentication code to be exposed.

E. Lost/Stolen PKI

In the event that, user lost his/her PKI or PKI has been stolen by an adversary. The adversary is still not able to gain any access, as only user's register mobile phone able to receive the short message containing one-time authentication code and obtain the proper WAP/GPRS page from the authentication server. Our proposed framework also requires user to acknowledge the choices "accept", which can only be done on mobile phone.

F. Phishing Attack Protection

Our two factor authentication prevents this via two different channels. Let's say the attacker able to pass the first level of authentication, but it will definitely not able proceed to the second authentication stage as only registered user mobile phone able to receive the SMS with an authentication code. If fraud has been taken place, this framework allows user to disallow the connection through the SMS. Besides that, user can select an option on mobile phone that will lock his/her account until further notice.

G. Lost/Stolen Mobile Phone

The security of this proposed framework is depending on the fact that user is in possession of mobile phone. We believe that this is a reasonable assumption, when people lose their mobile phones; they are typically reported lost and deactivated. Once deactivated, mobile will no longer be able to receive SMS messages destined for user.

H. Defense Man in the middle attack /Eavedropping

The security of this proposed framework is depending on the fact that user is in possession of mobile phone. We believe that this is a reasonable assumption, when people lose their mobile phones; they are typically reported lost and deactivated. Once deactivated, mobile will no longer be able to receive SMS messages destined for user.

IV. CONCLUSIONS

It is very important to ensure users who participate in cloud computing activities really have the identities they claim. The two-factor authentication framework proposed in this paper prevents unauthorized access to one's cloud services account at the very beginning stage. The first *PKI authentication* is an integration of public and private keys, digital certificate, digital signature and trusted third party CA security elements, which cooperate to provide a strong and reliable authentication medium. Only registered users with valid certificates will be authorized by the cloud authentication server and allowed proceed to the second step of *mobile OOB authentication*. NLM-128 generator is used here to generate an unpredictable session keystream and is subsequently sent to the user's mobile phone via a secure OOB channel. This one-time random code will only valid for a single session, thus protecting users from known phishing and replay attacks efficiently. The purpose of implementing two-factor authentication platform is to make it more difficult for attackers to gain unauthorized access to the cloud services.

ACKNOWLEDGMENT

This research was supported by the 2010 National Research Foundation Project and 2009 Dongseo Frontier Project.

REFERENCES

[1] Seny Kamara and Kristin Lauter, "Cryptographic cloud storage," in Proceedings of Financial Cryptography Workshop on Real-Life Cryptographic Protocols and Standardization, [Online] Jan 2010, [2010 May 29] Available: http://research.microsoft.com/pubs/112576/crypto-cloud.pdf

[2] John W.Rittinghouse and James F.Randsome, "Cloud Computing Implementation,Management and Security " in CRC Press, pp. 153-154, [Online] 2010, [2010 May 29].

[3] Frank Gens, "New IDC IT Cloud Services Survey: Top Benefits and Challenges in cloud computing," [Online] Dec 2009, [2010 May 29] Available: http://blogs.idc.com/ie/?p=730

[4] David Chou,"Strong User Authentication on Web," in Microsoft: The Architecture Journal, [Online] August 2008, [2010 May 29] Available: http://msdn.microsoft.com/en-us/library/cc838351.aspx

[5] Barney Beal, "Salesforce.com, customers hit with phishing attack," in SearchCRM.com, [Online] Nov 2007, [2010 May 29] Available: http://searchcrm.techtarget.com/news/1281107/Salesforce-com-customers-hit-with-phishing-attack

[6] Kaufman, L.M., "Data Security in the World of Cloud Computing," in Magazines of IEEE Security & Privacy, vol. 7, pp. 61-64, Jul 2009.

[7] Felician Alecu, "Security Benefits of Cloud Computing," in International Conference on Security for Information Technoloy and Communication, ISBN 978-606-505-137-9, pp. 71-76, Nov 2008.

[8] Cloud Security Alliance, "Top Threats to Cloud Computing V1.0," in Cloud Security Alliance Report, [Online] Mar 2010, [2010 May 27] Available: http://www.cloudsecurityalliance.org/topthreats.html

[9] Fujisawa, S., Otani, M., and Watanabe, K., "Implementation of PKI Authentication Functions for Network User Authentication System "Opengate"," in International Symposium on Applications and the Internet (SAINT), pp. 297-300, Jul 2008.

[10] Toorani, M. and Shirazi, A.A.B., "LPKI - a Lightweight Public Key Infrastructure for the mobile environments," in 11th IEEE Singapore International Conference on Communication Systems (ICCS), pp. 162-166, Nov 2008.

[11] W. Stallings, Cryptography and Network Security, 4th ed., Pearson Education, 2005.

[12] Hoon Jae Lee and Sang Jae Moon, "On an improved summation generator with 2-bit memory," in ACM of Signal Processing, vol. 80, pp.211-217, Jan 2000.

[13] T. Chang, B. Park, and Y. H. Kim, "An Efficient Inplementation of the D-Homomorphism for Generation of de Bruijn Sequences," in IEEE Transactions on Information Theory, vol. 45, pp. 1280-1283, May 1999.

[14] T. Chang and I. Song, "Cross-Joins in de Bruijn Sequences and Maximum Length Linear Sequences", in IEICE Transactions Fundamentals, vol. E76-A, pp.1494-1501, September 1993.

[15] HoonJae Lee, SangMin Sung, and HyeongRag Kim, "NLM-128, An Improved LM-type Summation Generator with 2-bit memories," in Proceedings of 4th International Conference on Computer Sciences and Convergence Information Technology (ICCIT), pp. 577-582, Nov 2009.

[16] Min Wu,Simson Garfinked, and Rob Mille, "Secure Web Authentication with Mobile Phones," in DIMACS Workshop on Usable Privacy and Security Software, 2004, [2010 May 29] Available: http://dimacs.rutgers.edu/Workshops/Tools/abstract-wu-garfinkel-miller.pdf
[17] Kandukuri, B.R., Paturi, V.R., and Rakshit, A, "Cloud Security Issues", in Preceedings of International Conference on Services Computing (SCC), pp. 517-520, Sept 2009.
[18] Daniele Catteddu and Giles Hogben, "Cloud computing: benefits, risks and recommendations for information security," in European Network and Information Security Agency (ENISA) 2009 Report, [Online] Nov 2009, [2010 May 27] Available: http://www.enisa.europa.eu/
[19] M. R. Pamidi, "Cloud Computing: A Status Report," in IT Newsletter of IT Newswire, [Online] Dec 2009, [2010 May 27] Available: http://www.itnewswire.us/Newsletter_December-28-2009.pdf
[20] Dai Yuefa, Wu Bo, Gu Yaqiang, Zhang Quan, and Tang Chaojing, "Data Security Model for Cloud Computing," in Proceedings of International Workshop on Information Security and Application (IWISA), pp. 141-144, Nov 2009.
[21] Ali Al-Qayedi, Wael Adi, Ahmed Zahro, and Ali Mabrouk "Combined Web/Mobile Authentication for Secure Web Access Control" in Proceedings of Wireless Communications and Networking Conference, 2004 [2010 May 29] Available: http://ieeexplore.ieee.org/stampPDF/getPDF.jsp?tp=&arnumber=1311267

Shirly Lee received her BS of Information and Science Technology, Honors Data Communication from Multimedia University, Malaysia in 2005. She is currently a master student in cryptography and network security lab at Dongseo University, Korea. From 2005 to 2007, she was an IT specialist at the Printelli Sdn Bhd Malaysia. She worked as IT Executive with Sunway Group, Malaysia in year 2007 till 2009. Her current research interests include Network Security and cryptography, Cloud Computing Security, RFID/USN security.

.

Ivy Ong received her BS of Information Technology, Honors Information System Engineering at Multimedia University, Malaysia in 2005. She worked as a software engineer II at Western Digital, Malaysia from 2007 to 2009. At present, she is pursuing the Master of Engineering in Graduate School of General at Dongseo University, Korea. Her research interests include hard disk drive technology, reliability analysis, mobile computing and network management.

HyoTaek Lim received his BS degree in Computer Science from Hongik University in 1988, the MS degree in Computer Science from POSTECH and the PhD degree in Computer Science from Yonsei University in 1992 and 1997, respectively. From 1988 to 1994, he had worked for Electronics and Telecommunications Research Institute as a research staff. Since 1994, he has been with Dongseo University, Korea, where he is currently a professor in the Division of Computer and Information Engineering. His research interests include computer network, protocol engineering, storage networking, IPv6 and mobile application.

HoonJae Lee received his BS, MS, and PhD Degrees in electronic engineering from Kyungpook National University, Daegu, Korea in 1985, 1987, and 1998, respectively. He is currently a professor in the School of Computer and Information Engineering at Dongseo University. From 1987 to 1998, he was a research associate at the Agency for Defense Development (ADD). His current research interests include developing secure communication system, side-channel attack and USN/RFID security.