International Journal of Smart Home
Vol.7, No.6 (2013), pp.333-342
http://dx.doi.org/10.14257/ijsh.2013.7.6.32

Design and Implementation of Reliable Content Transaction System in Smartphone Environment

Seng-Phil Hong[1], Sungmin Kang[2, *] and Jaejung Kim[3]

[1]School of Media and Information, Sungshin Women's University, Seongbuk-gu, Seoul, Korea
[2]The College of Business and Economics, Chung-Ang University, Dongjak-gu, Seoul, Korea,
[3]School of Media and Information, Sungshin Women's University, Seongbuk-gu, Seoul, Korea
[2]smkang@cau.ac.kr

Abstract

As the growth of the Internet has given consumers an access to unprecedented amounts of digital contents from almost anywhere, thanks to a variety of smart devices, it has raised concerns about the safety of personal data with current digital content transaction model when purchasing the online digital contents. Smartphone use is increasing rapidly and it is affecting every aspect of people's lives and working environment. Thus, smartphone has become an essential personal tool and individuals have much dependence on it. We examine the security issues of smartphone and smart work environment in terms of describing the threats and problems with respect to privacy information protection. In order to solve this problem, we propose a transparent and reliable online distribution infrastructure system equipped with improved protection of consumer rights, supplier revenue, and enhanced prevention of copyright infringement. To be precise, this secure digital content transaction system enables N-screen based consolidated authentication model from various smart devices to process transaction confirmation anonymously so that consumer's personal information can be protected. In addition, this anonymous authentication technology between user and service provider also allows possible security threats to be traceable by using traceable anonymous technology.

***Key Words**: PKI, User Authentication, Anonymous Technology, Digital Contents, Smartphone, Security Threats, Privacy Information Protection*

1. Introduction

The portion of smartphone was above 20% of the overall mobile phones in 2010 and it was expected to increase rapidly. It was estimated that the portion will reach about 40% in 2013. However, the number of smartphone users among the registered number of mobile telecom service customers already exceeded 50% in Korea. According to Korea Communications Commission, telecommunication industry showed that the total number of smartphone users in the domestic market is 28,337,000 by end of June 2012 among the 52,680,000 registered users of mobile telecom service users, taking the portion of 53.8%. And, it is projected that the number will soon exceed 30 million people the next month [1].

The growing trend of using smartphone in people's lives in terms of fun, communication, work, etc. are heavily affecting people's lifestyle and working environment of an organization [2, 3]. The smartphone enables communication, connectivity, content consumption, and content creativity. Thus, it is a tool that provides

[*] Corresponding Author

ISSN: 1975-4094 IJSH

an ability to support a wide range of social interactions since smartphone is a convenient, highly accessible, functional device that's developed to enable communication and further support creation of various multimedia content, whether it be video, audio, or text [4]. The smartphone is also effectively utilized in the work environment by developing and applying the useful applications for executing the business tasks. Smartphone can execute various procedures that are essential in business processes such as email, Internet searching, data management, *etc*.

Smartphone was started with the trend of unified communications which integrated telecom and Internet service in a single device format because it has combined the convenience of cell-phone portability with the computing and networking functions of PCs [5]. Shin and Shin [6] define smartphone as a next-generation mobile phone which consists of diverse functions including Internet information search capability, MP3, built-in camera, DMB (Digital Multimedia Broadcasting), GPS, and image information sending/receiving. Although, smartphone is regarded as an innovative personal and business tool, there are many security weaknesses associated with the smartphone. A smartphone can be easily exposed to the PC-level hacking and attacks by malicious code because smartphone users can freely download and install various applications and the frequency of wireless Internet access is highly incurring. There are a number of smartphone security issues that need to be analyzed and in this paper, we try to provide the innovative security framework for resolving the security threats that cause much damages regarding the bleach of privacy information and financial loss as a consequence. By identifying and analyzing a number of security threats in terms of specific problem statements, which describes the security issues in various areas of smartphone use with respect to user authentication, we suggest effective security controls and techniques to resolve the existing security problems. For this, we also conduct a simulation of our security framework to prove its effectiveness in resolving the security problems related to smartphone and smart work environment [7].

As the digital resources and network technology are rapidly progressing, a great amount of digital content applications are also being developed throughout the world. Expanded use of portable multimedia devices, in particular, such as smartphone, tablet PC, E-book reader is the major cause of this digital contents increment [8]. With the increased use of the Internet, the problem of collecting personal information excessively and its data leak has been on the rise from numerous web servers. Specifically, when purchasing online digital contents, it is required to strengthen protection of personal information and secure digital content transaction system safely.

In this paper, we suggest a safe and convenient digital content transaction system having function of consolidated authentication model that mobile device users can effortlessly use credentials in cloud computing environments. After this brief introduction, the reminder of this paper is organized as follows: Section 2 discusses the security issues in the current purchasing process of digital contents in smartphone environment. Then, we propose secure digital content transaction system using consolidated user authentication with anonymous certificate and accredited certificate is shown in Section 3. Section 4 describes overall prototyping of proposed system. Section 5 presents the comparison and simulation of our architecture. Finally, we conclude the paper and suggest the future research work in Section 6.

2. Related Research

2.1. Smartphone and Smart Work Environment Security

Choi [9] defines the smart device as connected device that enable the access of the Internet anywhere, anytime due to its features of portability and Internet access. It is different from PC in that it is not fixed at a single access point, it is on 24 hours a day, and it is carried as a personal device. He argues that smart device is a user centric device, which can add and change the necessary functions through the app store or market. Smart device leads the paradigm shift due to its characteristics of gathering and consuming the diverse forms of information through human and intelligent detection function. Smartphone is best regarded as this smart device. Choi [9] also argues that the smartphone security threats can be seen in types of loss, malicious code infection, information leak/data steal, financial loss, and attack others.

Security features and functions on the smartphone are weak mostly due to its diverse use areas. It can be easily attacked by hackers causing damages and bleaching privacy information. Even the financial damages can be incurred due to people's self-mistakes since operational errors can easily occur on smartphone by individual's misconception of the smartphone features and lack of protective measures to correct mistakes in using the smartphone. We often hear the cases of reported financial damages as a result of individual's mistake and lack of proper protective security measures.

The innovation of mobile telecommunication technology and use of the smart device have created a large change in business environment and this enabled smart work. Smart work was enabled by overcoming the limitation of office space through the utilization of various smart devices and IT. Thus, work could be done anywhere and anytime with efficiency by taking the advantage of smart work environment [10, 11]. Smart work is defined as a new business environment using the various information and communication technologies (ICT) including the smartphone and a future oriented business environment by overcoming the problems of existing business methods and pursuing the innovation [12].

2.2. Threats of Smartphone-related Security

The security threats associated with the use of smartphone can be attributed to wireless Internet access environment, openness of smartphone, open market of smartphone application, and theft & loss. Further, there are a number of malicious codes that create security threat of smartphone. Malicious codes can infect the smartphone through multiple access channels and points. Smartphone malicious codes are known as the codes that execute illegal actions of destroying the system and stealing the privacy information as it operates in smartphone. Most of the codes attacking the smartphone paralyzes the smartphone device functions, exposes the stored information in smartphone, and thereby tries to make the financial gain [13]. Security of wireless communication is weaker than that of wired communication. It is the same wireless communication but smartphone has a key feature of weaker security level in terms of H/W and S/W platform, network, application, device aspects than a general mobile phone. Since the smartphone is a publicly used OS based on open-source and API (Application Programming Interface) is provided in many cases, hacking is easily enabled through the worm and virus attacks from the information intruder perspective [2]. Smartphone has the feature that it is possible to use the software and content, which is provided in the open mobile environment, in addition to voice communication capability. Based on the these smartphone characteristics, five types of smartphone security threats in working environment of government bodies can be classified in to 1) tapping/eavesdropping, 2) information leak, 3) server attack, 4) device attack, and 5) other attacks based on social methods [14].

Using a smartphone implicates the high level of security risk. A smartphone has the characteristics of frequent application installation, on status in portability, and network connection/access. And, it can be argue that this raised the security risk of hacking and malicious code execution. [15] Further, there exists a vague anxiety about the security of smartphone due to the fact that not much time has passed since its first introduction. However, there could be many people who think that security level for smartphone banking is raised in comparison with earlier mobile banking since Korean smartphone banking regulations made the implementation of a variety of security technologies such as PKI-based digital certificate, keyboard security, antivirus vaccine, firewalls, etc. additionally mandatory. As seen by smartphone banking example, people's perception about the importance of security and its associated risk level are different [16]. Therefore, we need to examine the potential business problems of security threat on smartphone and smart work in order to provide relevant security measures to deal with them.

2.3. Problem Statements of Smartphone Security

Although the use of smartphone is rapidly growing and content market of smartphone is receiving an attention, individuals and firms are not well prepared for the security threats of smartphone, which became an alternate device to PC, and are voicing the concerns [17]. Especially, smartphone contains privacy information including the voice communication, received & transmitted message, phone numbers, location-based information, *etc.*, and has the possibility of privacy information exposal. Thus, the smartphone shows higher level of security danger than PC [18].

Smartphone usage and its application in work environment create a number of security weaknesses with respect to privacy information protection. There are many dangerous points where security threats contribute to personal and social damages in areas of business application, communication, information management, *etc*. In this section, we suggest a number of problem statements of smartphone security in various aspect of using the smartphone regarding privacy information protection.

We suggest the problem statements of smartphone security in personal use and business environment as the following. The key issue on smartphone security is regarding the user authentication in terms of using the device, accessing the contents, and using the relevant application, and engaging in SNS activities.

-Device Use: People easily lose their smartphone device and it becomes an easy target of theft. If proper PW protection on device itself and USIM chip are not applied to the smartphone, it is at a high risk of losing the privacy information and contents.

-Content Access: While engaging in business transactions and processing the information based on mobile office in smart work environment, there is a risk that confidential corporate information can be exposed and individual's privacy information such as id, pw and financial data can be easily stolen if protective security measure and controls are not applied. There should be proper access control on contents [19].

-Application Use: When using a smartphone application, proper user authentication procedure should be applied to identify exactly who is using the application and to keep track of the application usage information.

-Engaging in SNS: While exchanging the information and engaging in communication, people can expose much privacy information by error and by attacks of hackers and malicious codes. Also, individuals can easily expose other people's privacy information in terms of personal attack, witch-hunting, and simple slandering. Thus, it is important to correctly verify user authentication to monitor people's SNS activities.

It can be argued that in the period of IT convergence, software content is more important than hardware component, and content security of smartphone should be provided by considering both the software platform and infrastructure from the aspect of software lifecycle [17]. In order to promptly respond to smartphone security threat incident and resolve the problem, the efforts of establishing the collaboration system with related entities, developing the security technology, modifying security related policies, improving the user perception of security awareness, *etc.*, are essential [13].

In sum, we recognize that importance of security perception on smartphone is increasing with respect to its rapid spread. Thus, individuals should be more aware of the importance of security in terms of using the smartphone for personal and business purposes and taking precautions. Consequently, the government should provide relevant security policies and firms need to make active investments to protect organization's value information and assets.

2.4. The Current Digital Content Purchasing Process

Let us analyze the problems of current digital content purchasing process and suggest a secure transaction measure which would lead to the solution. In the existing transaction environment, content providers provide digital content to online service providers who actually sell the content to users. The problems of this model are as follows:

First, for the aspect of users, not only it can cause personal data spill but also it is hard to handle consumers' complaints promptly and appropriately. User authentication method is not provided variously either. Second, for the aspect of online service provider, security issues arise when collecting personal information, in addition to difficulties of managing conflicts with users, regarding content transactions. Third, for the aspect of content providers, the reliability of content purchase history is inadequate because they receive sales reports only from online service providers. Besides, it is difficult to protect content's copyright as well as burdensome to inquire consumer's information on purchase. [20].

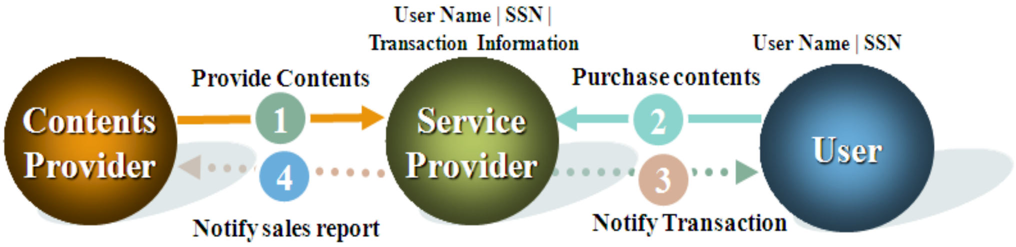


Figure 1. The Current Purchasing Process of Digital Contents in the Internet

In order to solve these problems, we proposed a transparent and reliable online distribution infrastructure which allows protection of consumer right and revenue of supplier, and prevention of copyright infringement.

3. Design of Secure Digital Content Transaction System

3.1. Overview

The secure digital content transaction system (SDCTS) consists of three components. The first is Consolidated Authentication Model (CAM) which is responsible for the N-Screen-based user authentication [8]. The second is Anonymous Certification Authority (CA) and Anonymous Trace Authority (TA). Anonymous CA takes a charge of issuance / disposal / verification of anonymous certificate to an anonymous user and provides a real name tracking function for illegal anonymous users with anonymous TA. Anonymous TA, on the other hand, manages a real name tracking function if service providers request a blindness tracking because an anonymous user misuses or abuses of anonymity [21]. Finally, the third is Content Manager which encourages a reliable online content transaction.

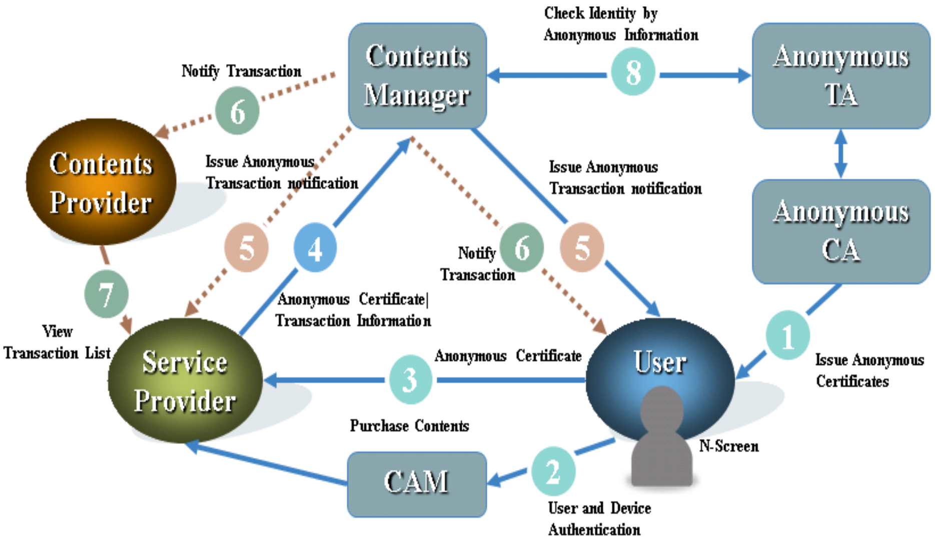

Check Identity by Anonymous Information
8
Contents Manager
Anonymous TA
Notify Transaction
6
Contents Provider
Issue Anonymous Transaction notification
Issue Anonymous Transaction notification
Anonymous CA
5
4
Notify
6
Transaction
5
7
Anonymous Certificate| Transaction Information
View Transaction List
Service Provider
Anonymous Certificate
User
1
Issue Anonymous Certificates
3
Purchase Contents
N-Screen
CAM
2
User and Device Authentication

Figure 2. System Workflow of Secure Digital Content Transaction System

The system workflow of secure digital content transaction system is as follows;

① Anonymous CA → User: Issue Anonymous Certificate
② User → CAM: Perform User and Device authentication
③ User → Service Provider: Purchase digital contents
④ Service Provider → Content Manager: Send transaction formation
⑤ Content Manager → {Service Provider, User}: Send transaction notification
⑥ Content Manager → {User, Content Provider}: Notify Transaction
⑦ Content Provider → Service Provider: View Transaction List
⑧ Content Manager → Anonymous TA: Check identity by anonymous information

3.2. PKI of Anonymity

Anonymous online transaction authentication service protects consumer's personal information by anonymously verifying transactions between online suppliers and consumers, and offers possible solutions through traceable anonymity when future disputes arise. [21] It also provides functions of anonymity, unforgeability, unlinkability, and exculpaability by means of group signature [22].

The procedure of the issuance of anonymous certificate through Anonymous CA (Key generation, Join) is as follows; Online service provider registered the group and items to Anonymous CA. User requests a group member key to Anonymous CA by generating digital signature using accredited certificate of user. Anonymous CA saves the trace information after verifying the validation of digital signature and sends the group member key to user.

The purchase procedure of content transactions is as follows;

Online service provider requests anonymous user to sign group signature. User generates and sends the group signature using group member key. Online service provider verifies the group signature through group public key from Anonymous CA. Content Manager delivers anonymous transaction list to online service provider, user, and content provider.

If the online service provider and Content Manager need an anonymous user tracking because of anonymity abuse the tracking procedure of user's identity is as follows;

Online service provider or Content Manager requests an anonymous user's identity to anonymous TA. Anonymous TA requests Accredited CA on the basis of the stored information in Anonymous CA. Accredited CA checks the identity and revoke the accredited certificate if necessary.

3.3. Consolidated Authentication Model (CAM)

In terms of the management and usage of credential (certificate, *etc.*), consolidated authentication model is divided into Consolidated Authentication Model using Smart Device (S-CAM using smart device of users and Consolidated Authentication Model using Credential Server (C-CAM) using centralized credential service.

S-CAM is a model which enables user mobile devices to perform N-screen based user authentication by using user certificate stored in the smart devices. This CAM does not need to install additional software such as plug-in or ActiveX in order to perform user authentication. It simply requires web browser such as Internet Explorer, Opera, Safari, Firefox, Chrome *etc*. Furthermore, this CAM is designed not to reveal the sensitive data such as digital signature information to authentication server through end-to-end encryption which ensures its secure delivery between Service Provider and Smart Device [23].

C-CAM, a consolidated authentication model using credential server, manages user credentials centrally at credential stores. If Terminal Unit doesn't possess credentials in own its storage user can choose two methods; one is that user can download them from credential server and create digital signature for user authentication, and the others is that user can request signing server to generate digital signature instead of user [24].

A variety of methods to perform user authentication [25] using CAM are as follows;

Case 1: In terms of S-CAM, when server requires user and device authentication from the user registered terminal unit, user performs user authentication through the credentials stored in user's smart devices.

Case 2: In terms of C-CAM, when server requires user and device authentication from the user registered terminal unit, user performs user authentication through the credentials stored in credential server and signing server generates proxy signature upon user's request.

Case 3: In terms of C-CAM, when server requires user and device authentication from the user registered terminal unit, user downloads the credential stored in credential server and terminal unit generates digital signature to authenticate the user.

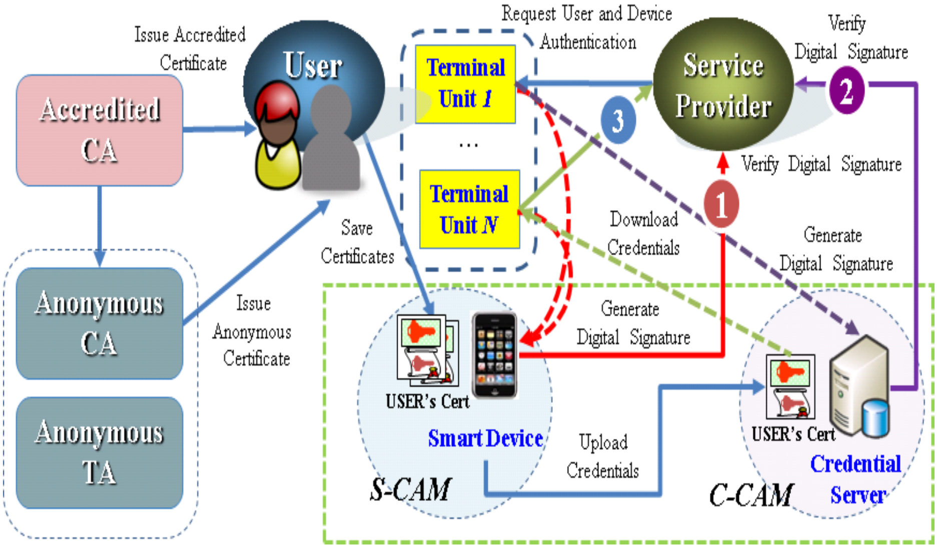
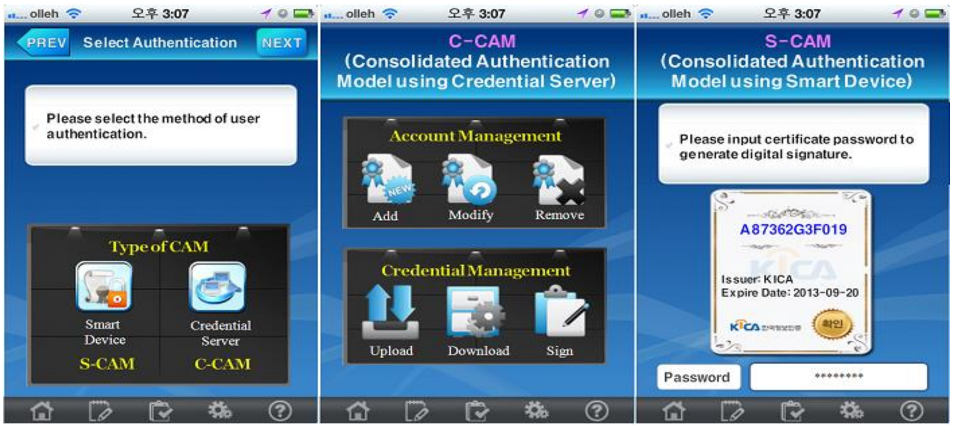


Figure 3. Consolidated Authentication Model

4. Prototyping and Implementation

To demonstrate the feasibility of our architecture, we implemented a prototype system which provides consolidate user authentication and anonymous authentication for secure digital content transaction system. This system is developed using JSP, JAVA, and iPhone development toolkit technologies. Figure 4 below shows CAM's login procedure using iPhone's Application.



Please select the method of user authentication.

Please input certificate password to generate digital signature.

Figure 4. User Interface for CAM in iPhone

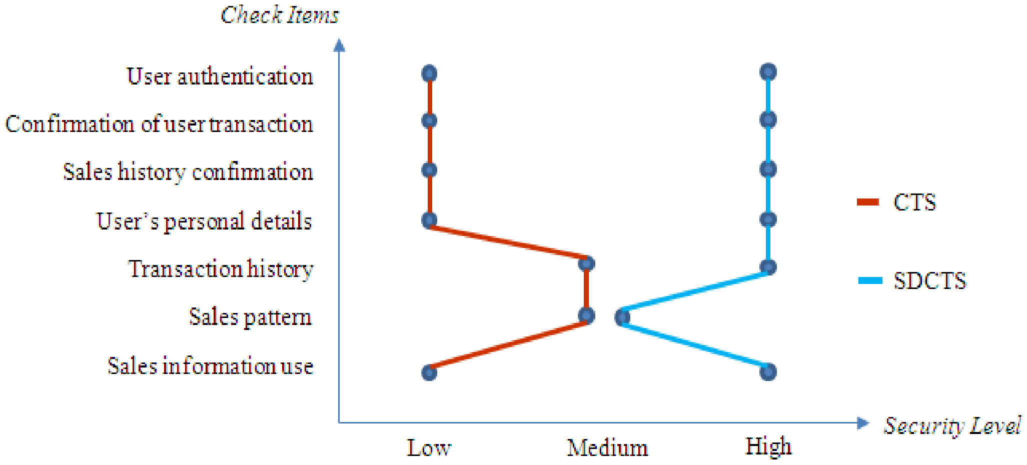
5. Comparison and Simulation

The secure digital content transaction system provides more secure and reliable infrastructure by solving the problem of exposing private information that exists in the current transaction services.

Table 1. Comparison between the Current Transaction Service (CTS) and SDCTS

Category	The current transaction service(CTS)	SDCTS
User Authentication	Authentication methods and mobile devices is limited	A variety of user authentication and N-screen based mobile devices are available
Confirmation of user transaction	Confirmed by the user's personal information	Confirmed by the user's anonymous information
Sales history confirmation of Content provider	Sales history contains the user's personal information	Sales history can be checked without user's personal information,
User's personal details	Personal information leak is possible	Personal information leak is impossible through anonymous authentication
Transaction history	Transaction history includes personal information	Transaction history includes anonymous information
Sales pattern	Individual buying patterns can be checked	Selective information according to consumer's choice is available
Sales information use	Impossible to use sales information due to personal information exposure	Anonymous information of sales pattern can be utilized in a range of business areas

The SDCTS provides a more reliable and secure transaction compared to the current transaction service as below;



6. Conclusions and Future Work

In this paper, we discuss the security issues of the current digital content transaction that are not able to provide personal information protection due to the absence of consolidated user authentication method. In order to solve this problem, we proposed the secure digital content transaction system so that one content is applicable to various mobile devices.

Following is contributions of N-screen based consolidated authentication model for the Internet services that designed the secure CAM architecture in cloud computing environments, which not only provides more flexible authentication framework but also leads to safer credential management in operating various mobile devices such as smartphone, smart pad, etc. In short, when this secure digital content transaction system combined with group signature based anonymous authentication technology is used first, online service provider can check user's sales history from anonymous information, second, content provider can check sales history without having to know personal information, and finally, user can prevent the leaking of their private data. At last, by protecting details of personal information, consumers' buying patterns and purchase information can be available to a variety of businesses. The future study will continue to focus on the design and implement of our suggested model, and we will expand it to new devices and environment.

Acknowledgements

This work was supported by the Sungshin Women's University Research Grant of 2013.

References

[1] http://www.hankyung.com/news/app/newsview.php?aid=2012070924401 ("Smartphone users exceeded the 50%").

[2] J. S. Kim and J. I. Lim, "National Institution's Information Security Management on the Smart phone use environment", Journal of the Korea Institute of Information Security and Cryptology, Korea Institute of Information Security and Cryptology, vol. 20, no. 6, **(2010)** December, pp. 83-96.

[3] J. S. Lee and H. S. Kim, "A Study on the Status of Smart Work and Facilitation Methods", Journal of Korean Association for Regional Information Society, Korean Association for Regional Information Society, vol. 13, no. 4, **(2010)** December, pp. 75-96.

[4] R. Beale, "Supporting Social Interaction with Smart Phones", Pervasive Computing, IEEE, **(2005)** April-June, pp. 35-41.

[5] C. Guo, H. J. Wang and W. Zhu, "Smart-Phone Attacks and Defenses", Proceedings of the Third Workshop on Hot Topics in Networks HotNets-III, San Diego, CA, USA, **(2004)**.

[6] Y. N. Shin and W. C. Shin, "A Security Reference Model for the Construction of Mobile Banking Services based on Smart Phones", International Journal of Fuzzy Logic and Intelligent Systems, vol. 11, no. 4, **(2011)** December, pp. 229-237.

[7] J. S. Moon and I.-Y. Lee, "Office Device Authentication and Authorization Protocol in Ubiquitous Office Network", Information Journal, vol. 14, no. 7, **(2011)** July, pp. 2271-2292.

[8] J. J. Kim and S. P. Hong, "One-Source Multi-Use System having Function of Consolidated User Authentication", YES-ICUC 2011, **(2011)**.

[9] E. H. Choi, "Security Threats of Smart Devices by Analyzing the Malicious Code Trend", Review of KIISC, Korea Institute of Information Security and Cryptology, vol. 21, no. 3, **(2011)** May, pp. 7-11.

[10] H. C. Lee, J. H. Yi and K. W. Sohn, "Security Threat and Measures for Smart Work", Review of KIISC Korea Institute of Information Security and Cryptology, vol. 21, no. 3, **(2011)** May, pp. 12-21.

[11] T. K. Kim, H. K. Seo and D. Y. Lee, "A Study on the Security Method for Smart Work", 35th Proceedings of Korea Information Processing Society-Spring, Korea Information Processing Society, vol. 18, no. 1, **(2011)** May, pp. 931-933.

[12] M. S. Jeong, D. B. Lee and J. Kwak, "Analysis of Security Threats and of Security Requirements of Smart Work", Review of KIISC Korea Institute of Information Security and Cryptology, vol. 21, no. 3, **(2011)** May, pp. 55-63.

[13] S. H. Suh and K. S. Chun, "Smartphone Security Threats and Security Countermeasures", TTA Journal, Telecommunications Technology Association, no. 132, **(2010)** November-December, pp. 44-48.

[14] J. Y. Kim and H. J. Kim, "A Study on Server Security for Secure Smartphone-based Work Environment of Government Bodies", Journal of Security Engineering, Security Engineering Research Support Center, vol. 7, no. 6, **(2010)**, pp. 683-692.

[15] M. Z. Rafique, F. Ahmed, M. K. Khan and M. Farooq, "Securing Smart Phones Against Malicious Exploits", Information Journal, vol. 15, no. 2, **(2012)** February, pp. 903-922.

[16] J. B. Kim and S. M. Kang, "A Study on the Factors Affecting the Intention to Use Smartphone Banking: The differences between the transactions of account check and account transfer", International Journal of Multimedia and Ubiquitous Engineering, vol. 7, no. 3, **(2012)** July, pp. 87-96.

[17] J. S. Sung, "A Study of Contents Secure in Smart Phone", Journal of Security Engineering, vol. 8, no. 6, **(2011)** December, pp. 665-671.

[18] S. Y. Song, "Smartphone Facilitation Methods and Information Security", Newstomato, **(2011)**.

[19] Z. Chen, "Security of Mobile Transaction Electronic Ticketing", Information Journal, vol. 15, no. 6, **(2012)** June, pp. 2593-2598.

[20] S.-J. Moon, "A Suggestion for a New Reliable Real-Time Nested Transaction Model", Information Journal, vol. 14, no. 5, **(2011)** May, pp. 1579-1594.

[21] S. Lee and B.-H. Chung, "Pseudonym-based Anonymous PKI with Short Group Signature", ETRI, **(2009)** October.

[22] D. Boneh, X. Boyen and H. Shacham, "Short Group Signatures", CRYPTO 2004, LNCS 3152, **(2004)**, pp. 41-55.

[23] J. J. Kim and S. P. Hong, "A Consolidated Authentication Model in Cloud Computing Environments", International Journal of Multimedia and Ubiquitous Engineering, vol. 7, no. 3, **(2012)** July.

[24] C. Popescu, "A Secure Proxy Signature Scheme with Delegation by Warrant", Studies in Informatics and Control, vol. 20, no. 4, **(2011)** December.

[25] J. J. Kim and, S. P. Hong, "A Method of Risk Assessment for Multi-Factor Authentication", Journal of Information Processing Systems (JIPS), **(2011)** April, pp. 187-198.

**Corresponding author: Sungmin Kang, Ph.D., Professor
College of Business and Economics, Chung-Ang University
156-861, Heukseok-dong, Dongjak-gu, Seoul, Korea
E-mail: smkang@cau.ac.kr