Design of User Information Profiling for Consolidated Authentication in N-Screen Environment

Jae-jung Kim* , Seng-phil Hong**, Yu-jin Shin, Hyun-mi Jang and Jaehyoun Kim

School of IT, Sungshin Women's University, Computer Education, SungKyunKwan University, Seongbuk-gu, Korea

jajukim@hotmail.com, {philhong, zibeline, nicemiya}@sungshin.ac.kr, jhkim@skku.ac.kr

Abstract

There has been an increase in the services and contents based on heterogeneous multiple media in the wake of the emergence of various smart devices. However, it is difficult to share the services and contents because the smart devices adopt independent OS. HTML5 has come under the limelight which provides the interoperability and can solve such a problem. Nonetheless, the standardization for HTML5 has yet to be completed, making it difficult to achieve the integrated authentication for safe use of services. This paper presents the user profile design method for the integrated authentication within the service based on HTML5. We intend to discuss the measure which enables the integrated management of personal information within the heterogeneous devices using the designed integrated user profile information and can help provide the authentication by phase depending on the selection of user.

Keywords*: Consolidated Authentication, N-Screen, User profile, HTML5*

1. Introduction

The pattern of media content consumption is changing fast amid the rapid expansion in the use of connected devices. Wired and wireless internet technologies have been practically applied in our lives, and therefore an environment is required which allows the personalized content to be provided via heterogeneous devices anywhere without any constraint in the space. According to the IDC, the market research organization, the 916 million units of connected devices were released in 2011 worldwide, and their sales amounted to $48.9 million in the same period [1]. In 2014, approximately 1.5 billion units of connected devices are expected to be released [2]. Along with that, the market for the M-payment service using the smart devices is expected to grow at a rate of 67.8% for the next 5 years from 2010 [3]. (See the Figure 1).

*First Author, **Corresponding Author

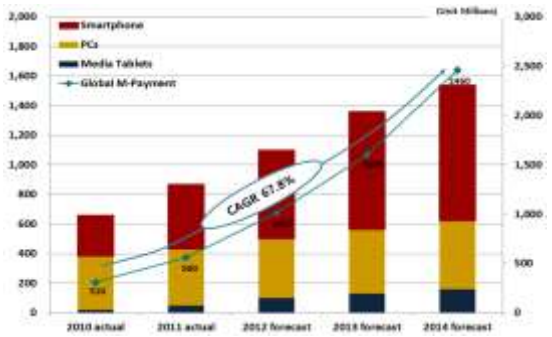

Figure 1. The Connected Device Forecasts in 2010-2014E

An increasing number of users have the desire to use the OSMU (One Source Multi Use) service based on the N-Screen owned by the user who has a single content amid the widespread use of smart devices, the increase in the heterogeneous media-based media, and rapid expansion of the smart mobile payment service. N-Screen refers to the service that provides the contents via several device screens, while OSMU is the method for using the contents without disruption by shifting single contents through several devices. However, the sensitive private information – which is necessarily involved in the use and sharing of single content on the basis of various heterogeneous multiple devices – is being managed sporadically based on the devices that have different platforms. This paper presents the method for the design of private information profile which is integrated using the HTML5.0 capable of flexibly responding to the compatibility, accessibility and interoperability based on different heterogeneous devices and the method for the application of authentication.

2. Problem Statement

Heterogeneous multiple devices, which can be easily carried, enable easy banking, transaction of securities, payment and financial settlement anytime and anywhere. Resultantly, there has been the difficulty in the authentication procedure and management that uses the private information, the essential information, due to the different platforms of heterogeneous media, and consequently, the problem of sporadic management and difficulty in management of private information have been witnessed.

- Absence of the technology that can be applied to ensure uniform integration and management of private information for heterogeneous devices
- Development of multiple authentications to cope with the diversification of user terminal device, version management, increase in the maintenance and repair costs
- Increasing inconvenience in managing the authentication information based on the heterogeneous media due to the dependent technology of browser and platform

3. Design of Consolidated Authentication Model (CAM) Profile

3.1. Overview of User Authentication Model (UAM)

We define that consolidated authentication model (CAM) can use in a variety of smart devices for user and device authentication. In terms of the management and usage of credential, CAM is divided into smart device based consolidated authentication model (S-

CAM) using smart device of users and credential server based consolidated authentication model (C-CAM) using centralized credential service.

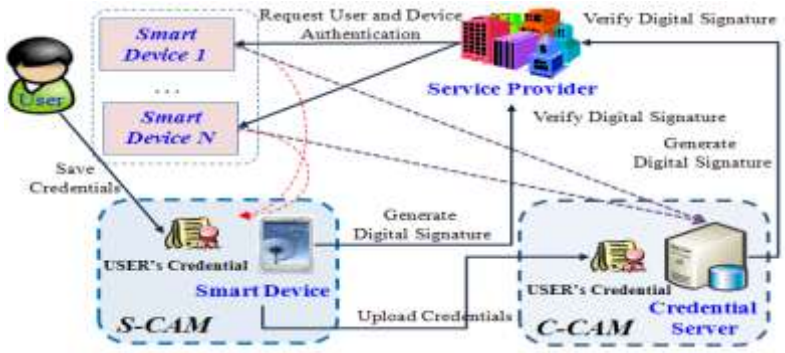

Figure 2. The Architecture of Consolidated Authentication Model

3.2. Smart Device based User Authentication Model (S-CAM)

The smart device based consolidated authentication model is a model which enables user smart devices to perform N-screen based user authentication by using user credential stored in the smart device. The structure and workflow of S-CAM is as follows; User saves a credential at smart device. If service provider requests user authentication user uses credential stored at smart device in order to generate digital signature. S-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. [4].

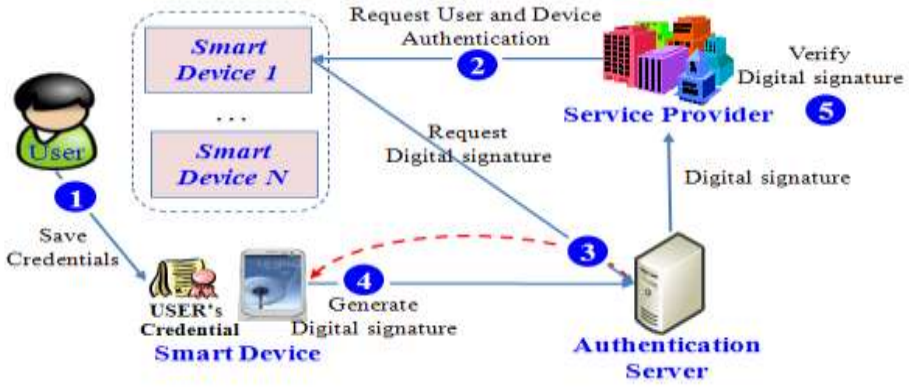

Figure 3. Structure and Workflow of S-CAM

3.3. Credential server based User Authentication Model (C-CAM)

The credential server based user authentication model manages user credentials centrally at credential stores. If service provider requests use authentication user can request to signing server which generates digital signature instead of user [5].

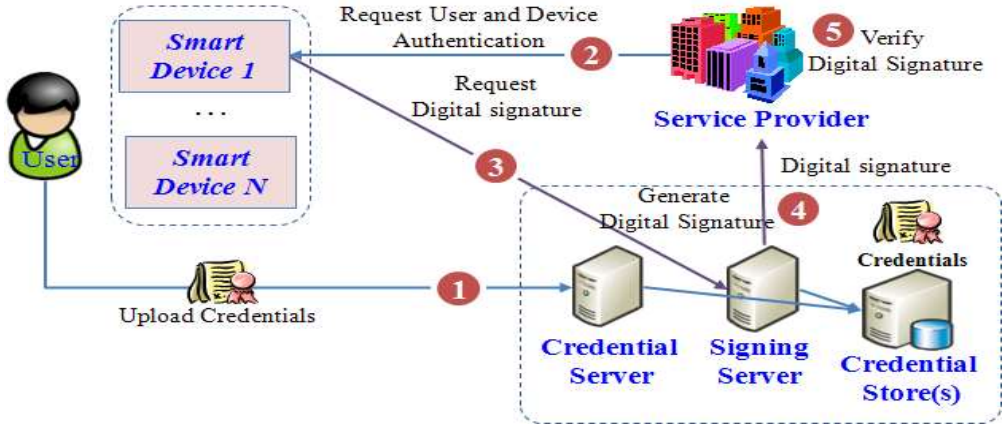

Figure 4. Structure and Workflow of C-CAM

3.4. Design of CAM profile

We design a common user authentication profile for consolidated user authentication. This profile consists of user information, smart device information, credential information, and policy information. User information field includes common user information such as social security number, name, email, phone number and ID. Device information field includes device type, name, serial number, phone number, MAC address, product ID and performance information. Credential information field includes CAM type, C-SAM information, S-CAM information, credentials, and secured credential. Policy information field includes and authentication level, authentication method, device authentication, content type and content level.

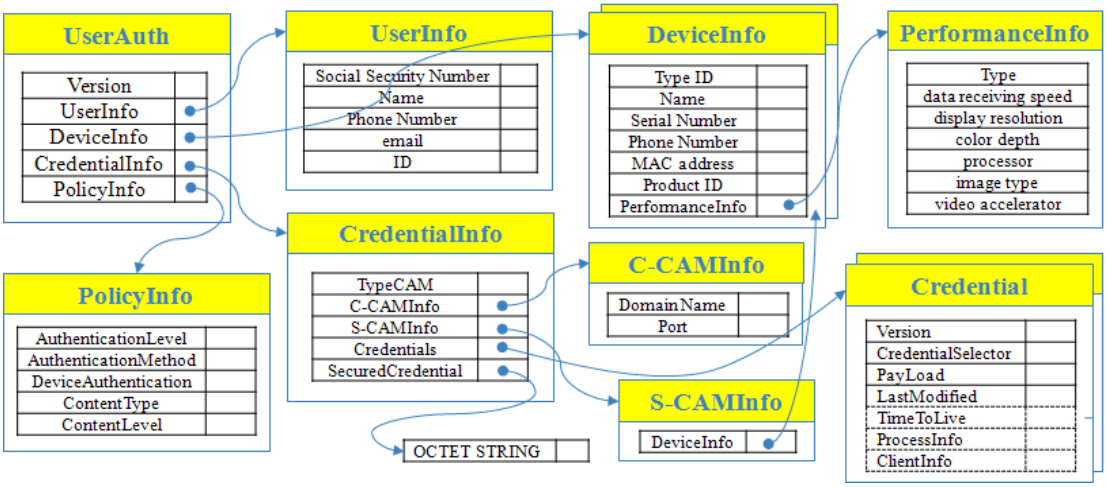

Figure 5. Profile of CAM

4. Prototyping

4.1. Implementation

Figure 6.User Profile Setting View

Figure 7. Android View (Login)

Figure 8. iPhone View (Alert)

Figure 6 is user profile setting view for user and device authentication in N-Screen environment. In this view, system manager can separate authentication level by setting user and device information. Also, manager can set the number of information which is used to each level. User and Device information can be set differently according to type of service, such as login, modify user information, and payment.

Figure 7 and Figure 8 is consolidated authentication view in mobile web browser. Through mobile web, user can use same consolidated authentication service in N-Screen environment. Figure 7 is Android, Figure 8 is iPhone. In the Login Page, user can set consolidated authentication level. If user set this level, System will notify level information to user. This notice includes user and device information type, which is used to consolidated authentication.

4.2. Simulation

Figure 9 is result of simulation. We simulate speed of service response. Graph A is result of service response time which is using user profile consolidated authentication system. Graph B is result of service response time which uses general consolidated authentication system. Graph C is result of service which is not using consolidated authentication system.

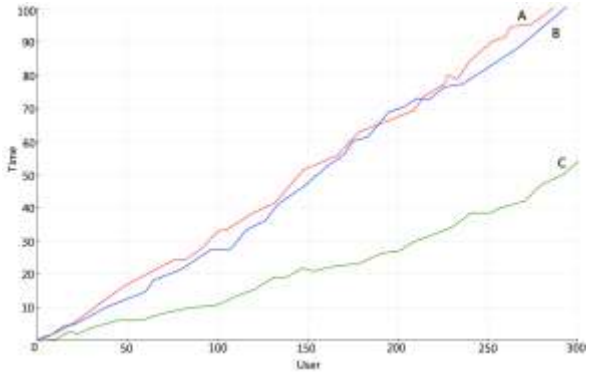

Figure 9. Simulation Result

As a result of simulation, service response time of A and B are very similar. Through this result, We can be ensured this system as not only security performance but also service response speed.

5. Conclusion and Future Work

In this paper, we suggest the design of consolidated authentication system which is using user profile. Through this system, we can use the strong consolidated authentication at HTML5 based service. The future study will continue to focus applying this system to actual environment.

Acknowledgements

This work was supported by the Sungshin Women's University Research Grant of 2012.

References

[1] National Information Society Agency (NIA), General Department of Information System Planning, IT Issues Weekly, **(2012)**.
[2] Y. -h. Lee, "Service Trends and Future Development Strategies of Domestic and Foreign M-Payment", The Banker, **(2011)**.
[3] S. -W. Lee, S. -M. Lee and J. -E. Oh, "Change and Opportunity of Smart Commerce", REAL Shipping, KT Economics Managements Research Institute, **(2010)**.
[4] J. -J. Kim and S. -P. Hong, "One-Source Multi-Use System having Function of Consolidated User Authentication", JCICT & The first Yellow Sea International Conference on Ubiquitous Computing (YES-ICUC) 2011, **(2011)**.
[5] 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.

Authors

Jae-jung Kim

Jae-Jung Kim received his BS degree in Computer Science from Chungnam University in 1997 and MS degree in Information Security from Korea University in 2003, respectively. Since 1997, he stayed in LG-CNS Systems and Korea Information Certification Authority Inc. to develop PKI solutions. And now he is undertaking a doctorate course as a member of the information security lab at Sungshin University. His research interests include Public Key Infrastructure (PKI), security architecture and protocol, cross certification, anonymous authentication, and device authentication.

Seng-phil Hong

Professor Seng-phil Hong received his BS degree in Computer Science from Indiana State University, and MS degree in Computer Science from Ball State University at Indiana, USA. He researched the information security for PhD at Illinois Institute of Technology from 1994 to 1997, He joined the Research and Development Center in LG-CNS Systems, Inc since 1997, and he received Ph.D. degree

in computer science from Korea Advanced Institute of Science and Technology (KAIST) in Korea. He is actively involved in teach and research in information security at The Sungshin Women's University, Korea. His research papers appeared in a number of journals such as ACM Computing, Springer-Verlag's Lecture Notes in Computer Science, etc. His research interests include access control, security architecture, Privacy, Smart Device Security and e-business security.

Yu-jin Shin

Yu-jin Shin received her BS degree in Computer Science from Sungshin woman's university. Currently she is studying for MS degree course at Sungshin Woman's university. And she is majoring in Information Protection. Her research interests include N-Screen, privacy, smart device security.

Hyun-mi Jang

Hyun-mi Jang received her BS degree in Industrial and Information Systems Engineering from Seoul National University of Science and Technology, and MS degree in computer science from Sungshin Women's University. Currently she is studying for her Ph.D. course at Sungshin Women's University, and she is majoring in Information Protection. Her research interests include access control, security architecture, and privacy.

Jaehyoun Kim

Professor Jaehyoun Kim received his B.S. degree in mathematics from Sungkyunkwan University, Seoul, Korea, M.S. degree in computer science from Western Illinois University and Ph.D. degrees in computer science from Illinois Institute of Technology in U.S.A. He was a Chief Technology Officer at Kookmin Bank in Korea before he joined the Department of Computer Education at Sungkyunkwan University in March 2002. Currently he is an associate professor at Sungkyunkwan University. His research interests include object-oriented modeling and design, software architecture, software process issues, and computer education.