User-based secure digital content durability service support OSMU

DaeHee Seo¹, MiYeon Yoon², DongSub Cho³, KabSeung Kou⁴, Jang-Mi Baek⁵

¹Electronics and Telecommunications Research Institute
²Korea Internet & Security Agency
³Ewha Womans University
⁴Infosec Technology Co. NRnD Team
⁵SoonChunHyang University

¹dhseo@etri.re.kr
²myyoon@kisa.or.kr
³dscho@ewha.ac.kr
⁴kabseung@infosec.co.kr
⁵bjm1453@sch.ac.kr

Abstract. The rapid advancement of the internet is changing in the form of knowledge information service. The previous service, which was the provider-oriented passive service model that supplies one-content from one device, evolves into the user-oriented active knowledge information service, therefore, the service provider provides the environment for the customers and the users create, distribute and manage the content based on various devices. Accordingly, a special service depending on each of forms is needed for mutual-sharing the information between various devices around the users. Therefore, in this study, for providing the digital content service between various user-oriented devices with the durability, by using the positional information of surrounding devices around the service provider and supplying mutual authentication service between the users, the device registered by the user in advance and the secured communication connection, we try to provide continuous service durability among various user-oriented devices.

Keywords: Digital Content, OSMU, Service Durability, User-oriented Service, Secure Communication

1 Introduction

The new internet environment represented as smartphone changes the user from passive service consumer to active producer and distributor. In particular, the service form that generates the information around the users and various devices is represented as a new socially/nationally important service. This kind of service is represented as a social network service, and provided from simple web-based environment to app environment in mutually-dependent relationship among individuals [1][6]. Therefore, the users have a strong point in escaping from the limitation to time and space, while the service compatibility among devices becomes
a problem since the fragmentary services are provided to each of the devices separately. Accordingly, the concept of OSMU (One Source Multi Use) for diversification of user devices is suggested and the method using codec-based service SVC (Scalable Video Codec) and middleware for utilizing it to various devices based on one digital content is now being researched [4][9]. In this method, the limitation of actual application is pointed out since it involves the need of special modification on the existing devices. Therefore, propose scheme in order to provide the service durability to the user in utilizing the constructing objects for providing the service, not the method using special modification on equipment or special device.

The second section of this study analyzes the technology summary for guaranteeing the service durability. The third section suggests the security requirement for user-based secure digital content durability service supports OSMU. The fourth section proposes the user-based secure digital content durability service supports OSMU. The fifth section analyzes the securely and efficiency of the proposed scheme and finally in the sixth section, the conclusion.

2 Technical analysis

According to the recent popularization of smart phone, the mutual communication and various devices are used around the users. Especially, cloud service for applying one service to various devices and OSMU is providing the service that is different from the existing one. In cloud service, the software and relevant data is hosted to central server by using SaaS (Software as a Service) and the user is utilized in the form of software delivery connecting through the client. This is the extension form of the existing ASP (Active Server Pages), focusing on the optimization on the scalability and the requirement by providing the service for unspecified individuals [11]. OSMU, by using one service or concept in various forms, can diversify the yield structure and for the users, they can be provided with various services from the surrounding devices[10], along with this, the research for providing the continuity of digital contents to various devices through SVC is ongoing [3][7]. Thus, the portability research on the digital content is the necessary research in user-oriented network, therefore, lots of studies are ongoing right now[12]. However, the problems are pointed out that there needs to construct special hardware outside of the existing digital content service continuity, there is a limitation to generating digital content or there needs to modify the existing digital content.

3 Analyzing on the security requirement

This section analyzes the security requirement for user-oriented secure intelligent service recognition,

- User authentication: If the existing ID method is used, a new variable value should be generated and be used to the authentication. A certain level of complexity and renewal needs to be possible and the method that can strengthen the security level of authentication level should be provided.
- Data and channel security: For service durability, the transmitted data, apart from the existing network security protocol, should be based on the encrypted communication for the secure transmission of user’s privacy and transmitted data, and the transmission information should be able to be verified.
- Renewable Security: For service durability, the mutual authentication based on two-way communication is necessarily provided and in remote terminal, the data for providing the integrity to the transmitted data is supplied and the data is able to be verified.
- Service durability: For service durability, without the hardware or software modification among component objects, the service provided to user as it stands should be provided securely and persistently. Based on positional information among user-oriented various devices, it validates other devices around users and provides the current service based on time stamp, not the re-transmission of the service from the beginning without lag and device form.

4 User-oriented secure digital content durability service supports OSMU

4.1 Assumptions

- The surrounding devices are previously distributed as the unique value in order to have the characteristic of contraction function that has certain continuity.
- The user registers SP in advance and the positional information of surrounding device \([a, b]\), stores the information to their mobile device.
- The user and the surrounding devices share the initial shared-value \(P_i\) in advance.

4.2 System coefficient

The following describes the system coefficient for user-oriented secure digital content durability service supports OSMU
\[
\begin{align*}
*: \text{User}(u), \text{surrounding device}(M), \text{Service provider (SP)} \\
ID,: \text{Objects of ID} \\
t,: \text{Time stamp} \\
< e >: \text{Event message} \\
[e]: \text{Request message for event message} < e > \\
\text{Seq}: \text{Sequence of Digital contents} \\
h,: \text{Secure hash value} \\
r,: \text{Random number} \\
E(): \text{Encryption algorithm} \\
p,, q,: \text{Public key, private key pair} \\
H(): \text{Secure hash algorithm} \\
SK_{A-B}: \text{Session key of between A and B} \\
\text{Contents}\_ID: \text{Digital contents ID}
\end{align*}
\]
4.3 Protocol

[Step 1] Providing a secure multimedia service

The following process is conducted to provide the user with secure multimedia service

1. In order for the user to be provided with multimedia service, the user calculates the following and transmits $<e>$, $h_u$, $V_u$ to SP.

   $<e> = \{ID_u, Service\_Request, Contents\_ID, Seq, t_u\}$

   $h_u = H(ID_u||Seq||<e>||t_u)$

   $a = ID_u Seq + r_u$

   $V_u = E_{pu}(a||h_u||r_u)$

2. SP receives $<e>$, $h_u$, $V_u$ from the user, verifies user’s ID and multimedia content ID in the event message, decrypted $V_u$ as personal key.

   If the authentication is right, then generate the mutual authentication value as the following and send it to the user by using $a$, $r_u$.

   $\beta = |Seq - r_u|$

   $V_{sp} = E_{pu}(a^\beta||r_{sp})$

   $h_{sp} = H(ID_{sp}||r_{sp}||[e]||a^\beta)$

   After calculating the mutual authentication value to provide this, generate a response message $[e]$ to user’s multimedia content event message $<e>$ as the following:

   $[e] = \{ID_{sp}||Service\_Response, Contents\_ID, Seq, t_{sp}\}$

   SP sends the user the response message $[e]$ for providing user’s service and $V_{sp}$, $h_{sp}$ for mutual authentication.

1. After the user receives $[e]$, $V_{sp}$, $h_{sp}$ from SP, the user decrypted $V_{sp}$ as its personal key, extracts $(a^\beta||r_{sp})$, verifies the integrity of $h_{sp}[e]$ by ID$_{sp}$. If the verification is correct, the user is provided with the service by SP from service response message $[e]$ based on Contents_ID and Seq.

2. If all the process is correct, the user and SP generates session key $SK_{sp-u}$ as the following:

   $SK_{sp-u} = H(a^\beta||r_u \oplus t_{sp}||r_{sp} \oplus t_u)$

[Step 2] Communication with other devices according to user’s movement

As the user moves, it is the procedure that sends central SP the service form that the user is provided with in present and user’s positional information according to it with the communications among surrounding devices.

1. If the user wants to be provided with the durability on the service by using other surrounding devices, the user codes the secret information between the user and

---

$P_i$: User and surrounding device of initial sharing value

$\lambda$: Value of contraction function

$X$: Unique fixed value of contraction function
SP, the positional information \([a, b]\) of surrounding devices, which the user knows and the current provided content’s \(\text{Seq}'\), calculates a secure hash value \(h_u\), sends \(V_u\), \(h_u\), \(t_u\) to SP.

\[
V_u = E_{SK_{u \rightarrow sp}}(\lambda|ru - r_sp|, [a, b], \text{Seq}')
\]

\[
h_u = H(|r_u - r_sp|, [a, b])
\]

2. After SP that received \(V_u\), \(t_u\) decrypted \(V_u\) by session key \(SK_{sp-u}\), it calculates \(|g(r_u) - g(r_{sp})| \leq \lambda|ru - r_sp|\) and verifies the existence of arbitrary \(\lambda\) (see Theorem 1). If the verification is correct, since \(g(r_u)\) is continuous in the interval \(g:[a, b] \rightarrow [a, b]\) depending on the feature of contraction function, \(g(r_u)\) has a fixed point \(X\). Therefore, based on fixed point \(X\) and arbitrary \(\lambda\), in order to provide the durability on the service that the user is provided with now, it checks the positional information \([a, b]\) of surrounding device \(M\) that the user wants to be provided with from, calculates the service information provided to the user as the following and sends \(V_sp\), \(t_sp\) to the surrounding device \(M\).

\[
V_sp = E_{p_M}(ru||\text{Seq}'||X||t_sp)
\]

3. After the surrounding device \(M\) decrypted \(V_sp\) from SP as personal key, it extracts \(ru\), \(\text{Seq}'\), \(X\), \(t_sp\) and requests the information on the current service from the users.

Service Request

4. The user generates the event message \(< e_1 >\) on the currently provided service and sends it to the surrounding device \(M\).

\[< e_1 >= \{ID_u, Service Request, Contents ID _, Seq', tu\}\]

5. After the surrounding device \(M\) receives \(< e_1 >\) from the user, generates the response message \([e]\), it calculates \(V_m\), which encrypted an arbitrary random number \(r_m\) and the positional information \([a, b]\) for setting the session key, \(\text{Seq}''\), the next sequence of \(\text{Seq}'\) of \(< e_1 >\) as public key of SP and sends \([e]\), \(V_m\), \(t_m\) to SP.

\([e] = \{ID_m, Service Response, Contents ID, Seq'', tu\}\)

\[
V_m = E_{p_M}(r_m||X||[a_1, b_1])
\]

6. SP receives event response message \([e]\), decrypted \(V_m\) as personal key, checks \([a, b] = [a_1, b_1]\) whether it corresponds to fixed point \(X\) and stores it corresponding to fixed point \(X\) one-to-one. After, SP generates \(SK_{M-U}\) for providing contents between the surrounding device \(M\) and the user, encrypts \(SK_{M-U}\) and Seq information by user’s public key and sends \(V_u\), \(V_M\) with time stamp \(t_sp\) separately.

1. \(SK_{M-U} = (X||r_m||ru)\)

A. \(V_u = E_{pu}(SK_{M-U}||\text{Seq}'' \oplus \text{Seq}')\), \(V_M = E_{pm}(SK_{M-U}||\text{Seq}'' \oplus \text{Seq}')\)

7. The surrounding device \(M\) which received \(V_M\), \(t_sp\) from SP decrypted \(V_M\) as personal key, extracts the session key \(SK_{M-U}\), switches the service corresponding to Contents ID as standby status for mutual authentication for transmitting it to the user by checking Seq. The user, after receiving \(V_u\), \(t_sp\), decrypted \(V_u\) as personal key, extracts the session key information and the content Seq and switches it to standby status for mutual authentication with the surrounding device \(M\).
5 Analysis on the proposed scheme

This section analyzes the user-oriented secure digital content durability service supports OSMU, which is suggested in the fourth section based on the security requirement suggested in the third section.

- User authentication: The proposed scheme, based on the existing ID and random number \( r_u \), generates \( ID_u \) and session key \( SK_{sp-u} \) after the mutual authentication with SP, by creating secured hash value \( h_u \) and \( a \). Therefore, it is possible to generate the variable value by the complexity of calculation involving ID and random number, so it enhances the security level.

- Data and channel security: This method generates each of session key \( SK \) for encrypted communication among each of objects by using data and channel security and provides the securely on transmitted data by using this. Also, it provides verifiable security service through the encrypted algorithm and hash algorithm to the information that needs the security such as user’s privacy data and positional information.

- Renewable Security: For service durability, it provides the integrity authentication of transmitted data from the remote terminal after conducting two-way explicit mutual authentication process by using \( H() \). In case of the positional information of surrounding device, it is verifiable through an arbitrary value \( \lambda \) that satisfies \( |g(x) - g(y)| \leq \lambda |x - y| \), \( (0 < \lambda < 1) \), originating from the contraction function.

- Service durability: For service durability, after it checks the positional information of the surrounding device of user by using the session key generated after the mutual authentication, it not only checks the next Seq’ of the current service Seq but also provides not only continuous service through time stamp for this if \( ([a, b] = [a_1, b_1]) \) is correct.

6 Conclusions

The recent broadcasting infusion environment changes the consumer from passive subject to positive and active subject that generates and distributes the information. Along with this, there are studies ongoing on the research of multiple OSMU usage based on one source if various smart devices construct the user-based network and provide the service; however, the studies are mainly focusing on the conversion of the digital content itself. Therefore, this proposed scheme is on user-oriented service durability that provides service continuity in terms of service, not the conversion of digital content itself. The proposed scheme verifies the positional information on other initially-registered devices of user and Seq on digital data and provides next Seq to one of the other devices that the user requires continuously. Thus, this method is differentiated from the method generating several sources and has a strong point that it is applicable to diversified devices if OSMU is applied. Henceforth, by expanding the proposed scheme in this study, we are going to construct the test environment involving SVC codec and realize it.
Acknowledgments. This research was supported by the ICT Standardization program of KCC Korea Communications Commission

References

12. ETSI TS 182 027 v2.0.0 (2008-02): Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IPTV Architecture; IPTV functions supported by the IMS subsystem.