International Journal of Security and Its Applications
Vol. 10, No. 9 (2016), pp.257-264
http://dx.doi.org/10.14257/ijsia.2016.10.9.24

A Secure Content Delivery Service in CPS Environments

Jin-Mook Kim[1], Jeong-Kyung Moon[2] and You-Jin Song[3*]

[1, 2]*Division of IT Education, Sunmoon University,*
70, Sunmoon-ro 221beon-gil, Tangjeong-myeon, Asan-si, Chungcheongnam-do, 31460, KOREA
[3]*Department of Management, Dongguk University,*
707 Seokjang-dong, Gyeongju, Gyeongsangbuk-do, 780-714, KOREA
[1]*calf0425@sunmoon.ac.kr,* [2] *moonjk1018@gmail.com,* [3] *song@dongguk.ac.kr*[*]

Abstract

Recently, smartphone and Wireless network environment is provided, users of IPTV services using smart phone is increasing rapidly. We want to method to collect and delivering of user's need, and to search for ways to securely transfer contents suitable. Moreover, if computing environment changes to CPS environment, these requirements are further increase. But, the suitable encryption algorithm and suitable secure protocol does not exist now. Therefore, we propose a new system to use the CP-ABPRE technique in order to safely transfer the contents in the CPS environments. Our proposed system can support to re-encryption and decryption on the smart gateway. It can provide to confidentiality, integrity, real-time response, and collusion attack resistance in CPS environments.

Keywords*: CPS, AB-PRE, Demand-on service, Smart TV, Content delivery service, Authentication*

1. Introduction

Since 2004, we used to smart-TV widely. Then, high-speed Internet service is provided to all. Therefore, the request of the IPTV service has increased using smartphones and smart TV. In order to connect the real world and the virtual world even more closely, many researcher studies of the cyber physical system and it is expanding widely now. Existing cloud computing services, the Internet of things technique has become a reality about CPS. This scheme make can support to collect and recommend the user friendly information to user [1].

In particular, CPS services within the next 15 years is expected to become a reality. Among them, IPTV service is the simplest service implemented using a smart phone. But, in order to transmit the content appropriate to the user's needs safely and quickly, often security requirements to be first solved.

Therefore, we use the CP-ABPRE techniques in CPS environment, I would like to propose a system that can secure content delivery in this study [2, 5, 6, 7].

2. Related Researches

2.1. CPS (Cyber Physical System)

CPS is a concept extends the conventional embedded system [4]. This have 3 major components such as Communication, Computation, and Control. This is modified to interact the existing embedded systems with the physical world. This is expected to

[*] Corresponding Author

ISSN: 1738-9976 IJSIA

develop into industry 4.0 model in the near future. For example, it looks like a smart grid, an internet of things.

With CPS environment well, we can have the advantages, such as improvement of productivity in the physical field, and reduction of the delay time for production. However, CPS environment as compared to conventional wired Internet environment can have a more serious security risks. Especially in CPS environment, it have been provided by the conventional wired Internet environment such as confidentiality, integrity, and availability service. Additionally, it must-have to timeliness and fault tolerance against of errors.

The following are three security requirements to be considered for the safe transfer content from CPS environment in this paper.

(1) Set of security keys such as master-key, session-keys

- SCP (Service and Content Protection) function must have a MAKE (Multi-Key Authenticated Key Exchange) protocol in CPS environments for provide a secure IPTV service. MAKE protocol must have a function for generating a session key from a master key in order to service users such as content provider, the authentication server, the smart gateway, end-user. Because, the IPTV service can provide a mutual authentication between end-user with another systems using this function. In particular MAKE protocol is used for encrypting or re-encrypting the attribute information collected by the sensors. For contents delivery system can support to user demanded-services.

(2) Re-encryption by Smart-Gateway

- There is a need a smart-gateway for researchers to provide a secure IPTV service. It exists between the authentication server and the user, a device which gives me performing proxy re-encryption or decryption. It is always necessary. Because the devices and sensors to be used in the CPS environment has only a low computing power. So, smart-gateway compute and accurate against of end-user's device or various sensors.

- In this case, smart-gateway performs the re-encrypted or decrypted by the agency using the CP-ABPRE technique.

(3) Low-weight encryption algorithms

- Always it needs a lightweight cryptographic algorithm to a number of sensors and terminals that exist in the lowest level in the CPS. We need a low-weight encryption algorithm because sensor and embedded devices have low computing power and low capacity. Therefore between smart gateway and sensor that must have minimum encryption algorithms to secure communication. It provide user’s recommended data by gathering at surround field. However, the encryption algorithm of the previously developed a public key infrastructure, it is difficult to use in a CPS environment. Because it is designed heavy, so it is difficult to use on the sensor device. To solve this problem, we developed the 128bit based LEA (Lightweight Encryption Algorithm) and LSH hash algorithm. And it is performed national standardization work.

2.2. CP-ABPRE [8]

Amit Sahai and Brent Waters introduced attribute-based encryption (ABE) as a new means for encrypted access control [5]. In an attribute-based encryption system ciphertext are not necessarily encrypted to one particular user as in traditional public key cryptography mechanism. But both users’ private keys and ciphertext will be associated with a set of attributes or a policy over attributes.

In their original system Sahai and Waters presented a Threshold ABE system in which ciphertext were labeled with a set of attributes S and a user's private key was associated with both a threshold parameter k and another set of attributes S0 [9]. In order for a user to decrypt a ciphertext at least k attributes must overlap between the ciphertext and his private keys. One of the primary original motivations for this was to design an error-tolerant (or Fuzzy) identity-based encryption scheme that could use biometric identities.

Pirretti *et al.* gave an implementation of the threshold ABE encryption system, demonstrated different applications of attribute-based encryption schemes and addressed several practical notions such as key-revocation. In recent work, Chase gave a construction for a multi-authority attribute-based encryption system, where each authority would administer a different domain of attributes. The primary challenge in creating multi-authority ABE is to prevent collusion attacks between users that obtain key components from different authorities. While the Chase system used the threshold ABE system as its underlying ABE system at each authority, the problem of multi-authority ABE is in general orthogonal to finding more expressive ABE systems.

Looking at the AB-PRE proposed by Hwa Jeong Seo [8], it can be classified as CP-ABPRE and KP-ABPRE. CP-ABPRE is a protocol to perform the re-encryption for user authentication and data transfer by attribute based on the proxy. This can enhance immediacy, security [3].

Hwa Jeong Seo's proposed CP-ABPRE model have 5 steps for re-encryption. This is Setup, GEN, RE-GEN, ENC, RE-ENC, and DEC. We know several CP-ABPRE model. They have a common point such as the following. The first common point, for users to re-encryption, perform a pre-registration to the authentication server. The second common point, to run the re-encrypted using the user attributes. And the third common point is, for real-time operation, to run the proxy encryption in response to the proxy delegation.

3. Proposed System

3.1. Construct of Proposed system

The proposed system has four components. In the proposed system, sensor collect user demanded information and it recommend to optimal content to the end-user using the sensor collected information. The proposed system has four components. In the proposed system, sensor collect user demanded information and it recommend to optimal content to the end-user using the sensor collected information. Then, The authentication server generate a plurality of session keys using the master keys. And the smart gateway re-encrypt and transmits the recommended content to the end-user using session key. Then the end-user decrypts the received secure content and listening to it. Figure 1 show components of our proposed system.

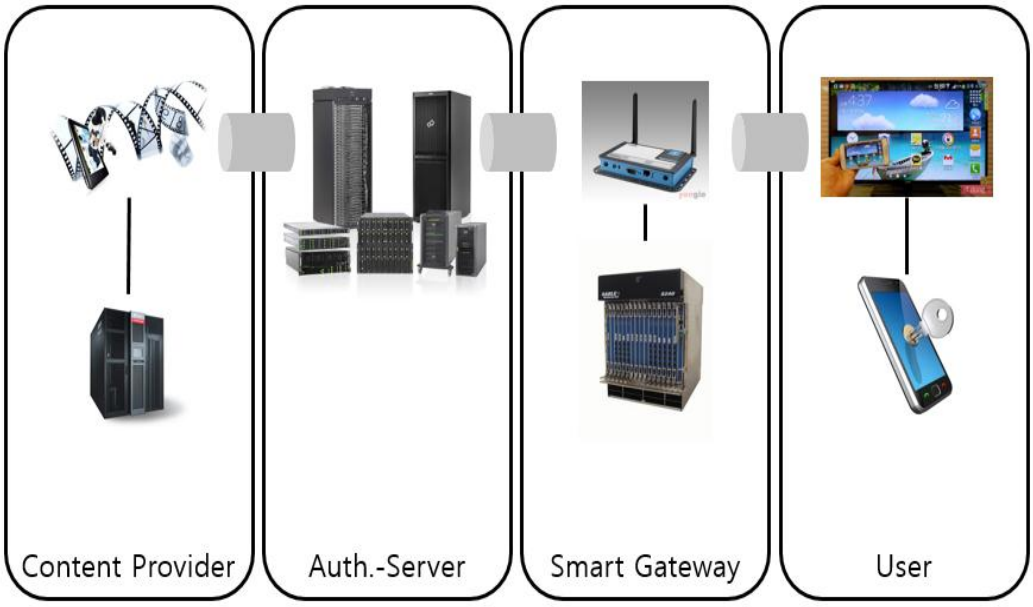

Figure 1. Components of our Proposed System

The first component of the proposed system is a content provider for providing a variety of contents. It is also included individuals broadcaster to a private broadcast as well as the broadcasting station. This is only registering their own identity information to be sure authentication server in the registration stage. The second component is an authentication server for content providers, smart gateway, users of the mutual authentication. Authentication server is a system that resist about content provider, smart gateway, and end-user, and it support access control by user's access rights and attribute.

In this study, we have limiting the authentication server to one. But, we have planning to authentication server extend in future research. The third component is a smart gateway. The smart gateway is the most important component in the present study. It is installed in a place where the home network or content provider has specified. And it is a device to perform re-encryption and decryption to end-user's smart-phone or smart-TV in order to transfer safely contents. The last component is a smartphone or a smart-TV. The end-user has it.

3.2. Proposed Scheme

Our proposed system have 6 step processing procedures. Proposed system designed by study of Haejeong Yoo and Hwa Jeong Seo to reference. This system is to search for content that is appropriate for your needs. In addition, the authority entrusted in the smart gateways re-encryption is performed safely delivered to the user. And end-user decrypts the received content and playing the content. It shows the operation of a proposed system in Figure 2.

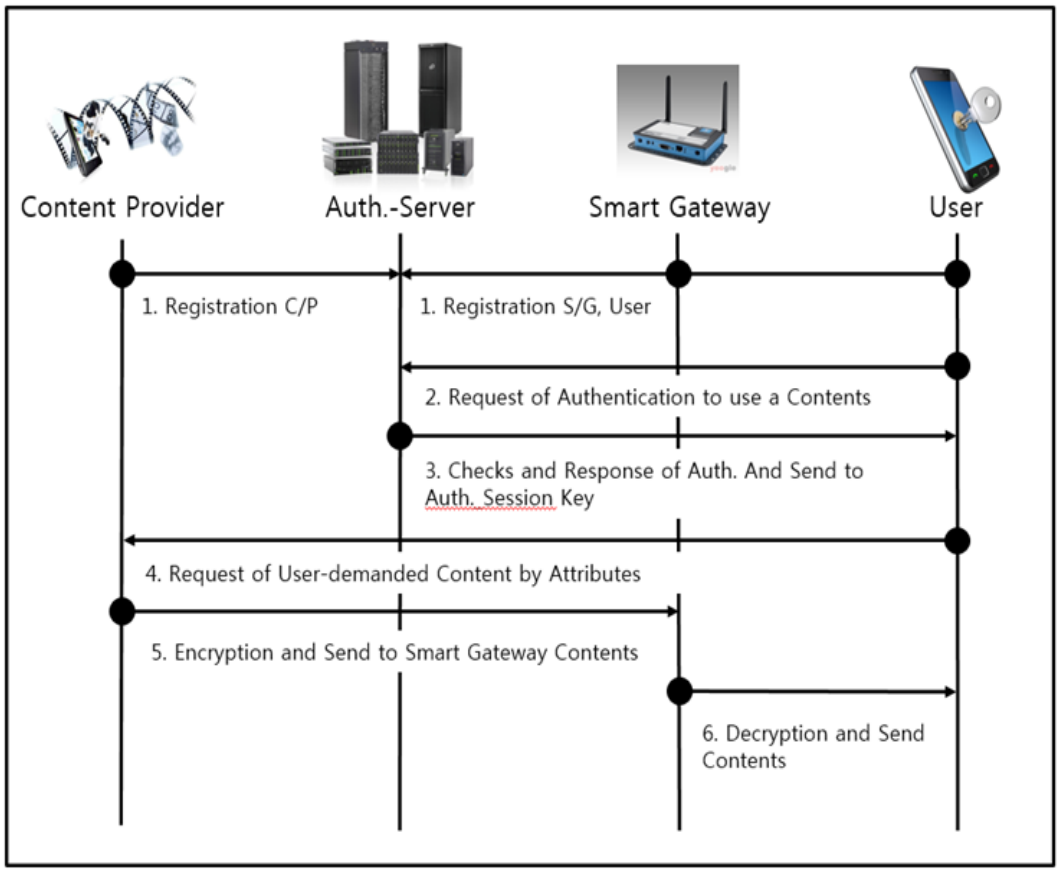

Figure 2. Procedures of our Proposed System

Our proposed scheme have 6 procedures.

(1) Registration step

- Each user make user-ID, and user-Password and registered it in the Authentication server. Authentication server generate Master-key using user-ID, user-PWD, and user-attribute information. Authentication server store it and transfer it to each user.

(2) Request of authentication step

- User send his/her Login information (user-ID, user-PWD, and user-Attribute) to authentication server. And request his access permission.

(3) Authenticate and Transfer session-key step

- Authentication server check user's login request, if right user want session key, authentication server generates session-key using user's attribute information and transfer session-key to right user for secure content delivery service.

(4) Request of Content step

- User request his want content to content provider or various sensor collect user's attributes such as location information, user's favorite information and so on and it send this information to content recommend system using user's attribute data.

- In this time, user use session-key and user's attribute data for secure content transfer.

(5) Encrypt and Transfer secure content step

- Content provider encrypt user requested content using session-key and lightweight secure algorithms between content provider and smart gateway. And transfer it to smart gateway system.

- Another side, if user want content using his smart-phone, he change his location data several time. Then content provider encrypt user wanted content using smart gateway session-key and transfer. And smart gateway decrypt it, and transfer to user it.

(6) Decrypt step

- User decrypt his received secure content from content provider using his attribute data and listen and show it. In this case, between smart gateway and user's smart-phone using lightweight decrypt algorithm because smart-phone or user side sensor have only low capacity.

4. Conclusion

Until now, we have examined the security requirements that are required by the CPS environment. And we proposed a new user authentication and re-encryption system suitable for CPS environment. The proposed system performs the re-encryption scheme on a smart-gateway using CP-ABPRE method.

The proposed system can solve the problem of security services that can be caused by low computational power having a conventional embedded system. In particular, the proposed system can provide fast and accurate encryption / decryption operations for mutual authentication using delegation techniques such as the attribute-based scheme. Therefore, the proposed system can provide a conventional security service such as confidentiality, integrity, and availability. As well as the proposed system is safe from password reuse attack, collusion attack. And the proposed system can provide the Multi-server mutual authentication required by CPS environment through further more study at future.

Acknowledgments

This research was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2013R1A1A2011581). This work was also supported by the Dongguk University Research Fund of 2015.

References

[1] R. S. Pippal, S. Tapaswi and L. Li, "Secure Key Exchange Scheme for IPTV Broadcasting", Informatica, vol. 36, no. 1, **(2012)**, pp. 47-52.
[2] I. Lin, M. Hwnag and L. Li, "A New Remote User Authentication Scheme for Multi-server Architecture", Future Generation Computer System, vol. 19, no. 1, **(2003)** March, pp. 13-22.
[3] H. Yoo, "Attribute based User Authentcation for Contents Distribution Environments", International Journal of Contents, vol. 8, no. 3, **(2102)** September, pp. 79-82.
[4] Y. Eun, K.-J. Park, M. Won, T. Park and S. H. Son, "Research Trend of Cyber Physical System", Communications of the Korea Information Science Society, vol. 31, no. 12, **(2013)** Dec., pp. 8-15.
[5] A. Sahai and B. Waters, "Fuzzy Identity Based Encryption", Proceeding of Eurocrypt'05, LNCS3494, **(2005)**, pp. 457-473.
[6] V. Goyal, O. Pandey, A. Sahai and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data", CCS'06, **(2006)** October, pp. 89-98.
[7] M. Green and G. Ateniese, "Identity-based proxy re-encryption", Applied Cryptography and Network Security, Springer Berlin Heidelberg, **(2007)**.

[8] H. J. Seo and H. Kim, "Attribute-based Proxy Re-encryption with a Constant Number of Pairing Operations", Journal of information and communication convergence engineering, vol. 10, no. 1, **(2012)** March, pp. 53-60.
[9] J. Bethencourt, A. Sahai and B. Waters, "Cihpertext-Policy Attribute-Based Encryption".

Authors

Jin-Mook Kim, He received the Ph.D in computer engineering, computer security and authentication from the Kwangwoon University in 2006. Currently, He is a assistant professor in the Division of IT Education at Sunmoon University in Korea. His research interests include network control architecture, security engineering, authentication on the network, and Smart-phone security.

Jeong-Kyung Moon, She received the MS degree in Electronic Commerce from Dankook University in 2006. And she received the PhD. Candidate in Computer science from College of Engineering / Kongju National University in 2013. She is a professor of Contract in Division of Information Technology Education, Sunmoon University currently. She's research interests includes Cloud Computing, Information security, Network security and Authentication.

You-Jin Song, He received the Ph.D. in Department of Information Security, Tokyo Institute of Technology University at Japan. He was work and researh about various security service and protocol at ETRI(Eletroincs and Telecommunications Research Institute) from 1988 and 1996 in Korea. He is a Professor in department of business and administration, Dongguk university Gyeongju Campus, Korea from 1996 and now. His research interest are Ubiquitous and IoT security services and Privacy , Digital content secure services, SCM/CRM sercrity services.