Advanced Science and Technology Letters
Vol.120 (GST 2015), pp.278-281
http://dx.doi.org/10.14257/astl.2015.120.56

Security Enhancement of Cloud Service in E-Navigation Environment*

Donghyeok Lee, Namje Park†

Department of Computer Education, Teachers College, Jeju National University,
61 Iljudong-ro, Jeju-si, Jeju Special Self-Governing Province, 690-781, Korea
{bonfard, namjepark}@jejunu.ac.kr

Abstract. The Maritime Cloud is the term used to describe the concept of an infrastructure that support authorized, seamless information transfer, as requested by the IMO e-navigation strategy, and as derived from testbeds focused on e-navigation. This paper proposes a lightweight user authentication protocol where the Message Queue Telemetry Transport type protocol registers unique topic values from the user to send the value to a server through the QoS(Quality of Service) 2 method and lightweight usage information measurement protocol where the transmission of usage information for communication service measurement consumes less mobile device resources.

Keywords: Cloud, E-navigation, IMO, Secure Maritime

1 Introduction

The IMO e-navigation strategy has requested a communication infrastructure providing authorized seamless information transfer between stakeholders. The Maritime Cloud is the term used to describe the concept of an infrastructure that support authorized, seamless information transfer, as requested by the IMO e-navigation strategy, and as derived from testbeds focused on e-navigation. The Maritime Cloud concept is similar to the maritime infrastructure framework, adding those elements, that are necessary to support the e-navigation domain.

A limited testbed version of the Maritime Cloud concept exists, which has so far demonstrated interoperable information exchange between systems developed by different e-navigation testbed projects in Northern Europe and Korea. Based on the experience of several e-navigation test bed projects in Europe (EfficienSea, MonaLisa, and ACCSEAS) as well as projects in Korea and Japan, the concept of the Maritime Cloud has been developed into an open source functional prototype.

* This work was supported by the Korea Foundation for the Advancement of Science and Creativity(KOFAC) grant funded by the Korea government(MOE). And, this research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education (2013R1A1A4A0 1013587)
† Corresponding author : Namje Park (namjepark@jejunu.ac.kr)

ISSN: 2287-1233 ASTL

2 User Authentication Protocol in E-navigation Cloud

The proposed system distributes unique topic values generated by combining a user timestamp, device number and random value among a Client-Gateway-Broker and server within in a reliable cloud server to the broker and server. Based on the distributed unique topic value, the server and broker check the integrity of the topic internally. Once checked, the server issues a usable secret value based on the unique topic value sent by the user, the user then combines the existing unique topic value with the sent secret value and sends a user authentication message to the server, and the server then validates the sent final value to finally register the user. Even if the unique topic value is hijacked during the process, the integrity is ensured through the timestamp the user generated and the random value assigned, which eliminates the possibility of reuse attacks.

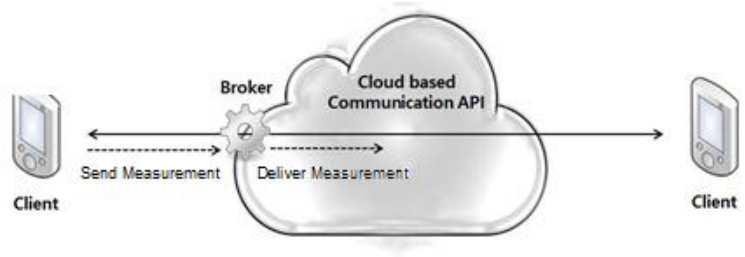

Fig. 1. Cloud Communication Process

Before being utilized in a Cloud-based communication service, a reliable user authentication process is performed among Client-Service Broker-Server to verify users. Table is a list of abbreviations used in the protocol for user authentication.

Abbreviation	Description
R_n	Random Number
T_n	Timestamp
h()	Hash Function
A_{TP}	Authentication Topic
S_{TP}	Secret Topic
C_{AK}	Client Access Ket

Fig. 2. Abbreviations used in Protocol

The client generates timestamp T_N to prevent reuse attacks with random value R_1 as (F. 1), and then generates unique topic value A_{TP} as (F. 2) based on random value R_N, timestamp and the device's unique PIN ID to register on the MQTT broker.

$$Generate\ \ R_N, T_N \qquad \text{(F.1)}$$

$$Generate\ A_{TP} = H(ID \| R_N \| T_N) \qquad \text{(F.2)}$$

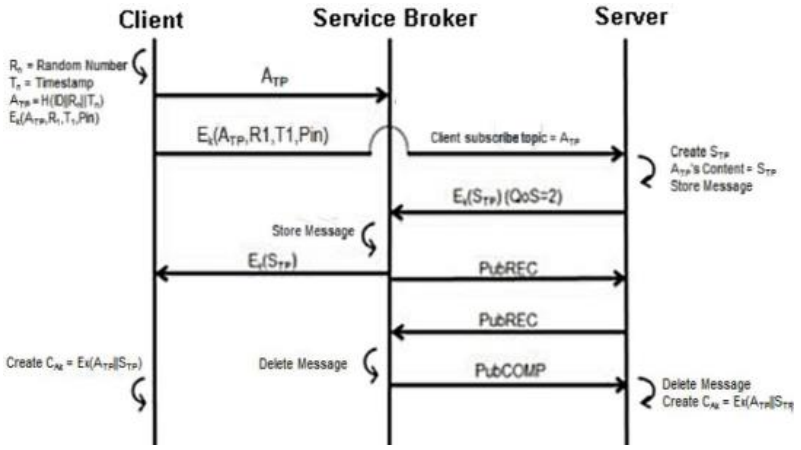

Fig. 3. Proposed User Authentication Protocol

3 Conclusion

This paper proposes a lightweight user authentication protocol where the protocol registers unique topic values from the user to send the value to a server through the QoS method and lightweight usage information measurement protocol where the transmission of usage information for communication service measurement consumes less mobile device resources.

To support the e-navigation strategy for global maritime transport, the Maritime Cloud offers a Maritime Identity concept for all participating stakeholders in a common framework. Information services for e-navigation will be published in a dynamic registry, available for discovery by relevant stakeholders. An opportunity for placing the Maritime Cloud Client Component (or Service Agent) into the ships bridge architecture exists in the ongoing standardization processes. While a window of opportunity for initializing the establishment of the Maritime Cloud exists, a governing structure, business model and operational environment with related evolutionary processes for cooperation amongst many different projects and stakeholders will have to be established for the Maritime Cloud (or maritime infrastructure framework) to ensure long term sustainability.

References

1. Jens K. Jensen, Mikael Lind, Kwangil Lee, Jin Hyoung Park, Per Setterberg : How the Maritime Cloud supports e-navigation. E-NAV16-Task 5.1.19 (2015)
2. Jens K. Jensen, Mikael Lind, Kwangil Lee, Jin Hyoung Park, Per Setterberg : A Maritime Infrastructure Framework. E-NAV16-9.24, Task 5.1.19 (2015)

3. Jeongho Kim : The weight of the mobile device user authentication protocol study the cloud service communications environment. Soongsil university thesis (2015)
4. Park, N.: Security scheme for managing a large quantity of individual information in RFID environment. In: Zhu, R., Zhang, Y., Liu, B., Liu, C. (eds.) ICICA 2010. CCIS, vol. 106, pp. 72--79. Springer, Heidelberg (2010)
5. Park, N.: Secure UHF/HF Dual-band RFID: Strategic Framework Approaches and Application Solutions. In: ICCCI 2011. LNCS, Springer, Heidelberg (2011)
6. Park, N.: Secure Data Access Control Scheme Using Type-Based Re-encryption in Cloud Environment. Studies in Computational Intelligence, vol. 381, pp. 319--327. Springer (2011)
7. Park, N., Kim, S., Won, D., Kim, H.: Security Analysis and Implementation leveraging Globally Networked Mobile RFIDs. In: PWC 2006. LNCS, vol. 4217, pp. 494–505. Springer, Heidelberg (2006)
8. Park, N., Kwak, J., Kim, S., Won, D., Kim, H.: WIPI Mobile Platform with Secure Service for Mobile RFID Network Environment. In: Shen, H.T., Li, J., Li, M., Ni, J., Wang, W. (eds.) APWeb Workshops 2006. LNCS, vol. 3842, pp. 741--748. Springer, Heidelberg (2006)
9. Kim, Y, Park, N., Hong, D.: Enterprise Data Loss Prevention System Having a Function of Coping with Civil Suits. Studies in Computational Intelligence, vol. 365, pp. 201–208. Springer (2011)
10. Park, N.: Implementation of Terminal Middleware Platform for Mobile RFID Computing. Int.J.Ad Hoc Ubiquitous Comput., 8 (2011) 205-219
11. Park, N.: Detection Experimentation and Validation of Web Applications using both Static and Dynamic Analysis. International Information Institute (Tokyo).Information, 18, pp. 1735 (2015)
12. Park, N.: Development and Application of Elementary STEAM Career Education Program using LOGO Programming and Fractals Learning. Advanced Science Letters, 2, 549-552 (2015)
13. Park, N., & Bang, H.: Mobile Middleware Platform for Secure Vessel Traffic System in IoT Service Environment. Security and Communication Networks, (2014)
14. Park, N., Park, J., Kim, H.: Inter-Authentication and Session Key Sharing Procedure for Secure M2M/IoT Environment. International Information Institute (Tokyo).Information, 18, 261 (2015)

