2020년도 한국통신학회 하계종합학술발표회

공개 키 암호화 시스템을 사용하는 ICN 기반 실시간 헬스 모니터링 시스템

하산 캄룰, 정성호

한국외국어대학교 정보통신공학과

An ICN-based Real-time Health Monitoring System using Public-Key Cryptosystem

Kamrul Hasan and Seong-Ho Jeong, Dept. of ICE, HUFS
kamrul@hufs.ac.kr, shjeong@hufs.ac.kr

Abstract

The real-time healthcare monitoring system will be helpful for our healthy daily lives. The most sensitive health-related data needs to be exchanged between the patient and the healthcare monitoring system in a secure manner. Information-centric networking (ICN) is a paradigm shift in the modern Internet architecture that provides packet-level security. Although several ICN-based healthcare systems are available, the ICN-based real-time health monitoring mechanism is still unavailable, and the offered level of protection is not sufficient for the healthcare system. In this paper, we propose a secure ICN-based real-time health monitoring system using public-key cryptosystem (PKC) to ensure the privacy and security of healthcare users based on a public-key infrastructure (PKI) mechanism.

I. Introduction

Real-time health monitoring is becoming a realistic demand due to the dramatic update of the healthcare system. The Information-centric healthcare system is seeking attention due to the inherent packet-level security of ICN. However, the ICN-based healthcare system involves a wide range of communication nodes that exchange sensitive data, which poses challenges to both security and privacy [1]. The PKI-based digital certificate infrastructure [2] can solve the security and privacy issues in the ICN-based real-time health monitoring system.

II. A Secured Healthcare Monitoring System

Figure 1 illustrates a potential real-time health management system model in which the patient manager controls the sensing and the co-ordination of patient monitoring information in real-time, e.g., blood pressure and cardiac and respiratory levels. The patient manager notifies the hospital servers of any emergency regarding the patient's wearable sensor devices data. A doctor in the hospital monitors the emergency server and responds to the patients, including medication.

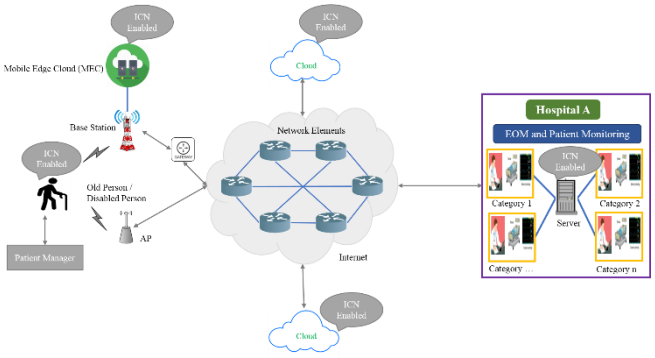

Figure 1: A real-time health monitoring system

The essential and emergency messages securely delivered to the hospital server based on the PKI mechanism. Figure 2 shows the detailed functional architecture of the PKI mechanism between a sender, e.g., a patient manager and a receiver, e.g., the hospital server. A PKI mechanism consists of several functionalities such as security policy, certification authority, registration authority, certificate repository and distribution system, and PKI-enabled applications. The certificate authority generates a public and private key for all patients and doctors, nurses, and respective employees of the hospitals. Figure 2 (a) and (b) shows that the patient sends the ciphertext of any message (M) based on the encryption algorithm using the receivers public key or senders private key. Upon receiving the ciphertext, the hospital server decrypts it using the senders public key or receivers private key. Every user knows the public key of other users, but the private key is unknown. Therefore, the privacy of the user is maintained, and the encryption mechanism also supports the security of the content.

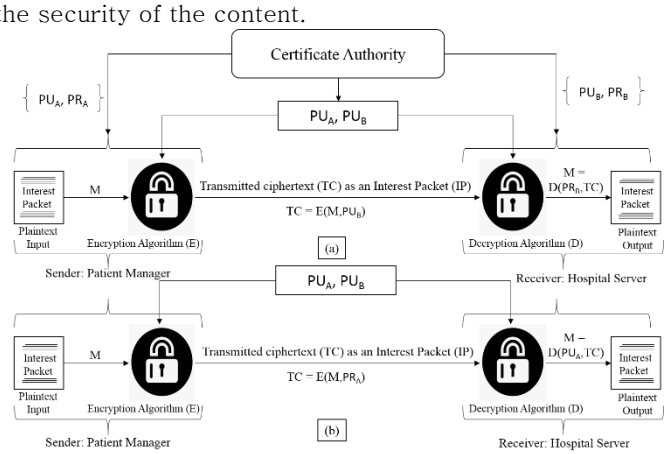

Figure 2: The security mechanism for the real-time healthcare monitoring system

III. Concluding Remarks

This paper primarily explained the architectural and functional description of the secured ICN-based real-time health monitoring system using the PKI mechanism. We also ensured the privacy and security of a patient and content in the proposed healthcare monitoring system.

Acknowledgement

This research was financially supported by the Ministry of Trade, Industry, and Energy (MOTIE) and Korea Institute for Advancement of Technology (KIAT) through the International Cooperative R&D program.

References

[1] R. Boussada, B. Hamdaney, M. E. Elhdhili, S. Argoubi, and L. A. Saidane, "A Secure and Privacy-Preserving Solution for IoT over NDN Applied to E-health," 2018 14th IWCMC COnference, Limassol, 2018, pp. 817-822.

[2] R. Hunt, "PKI and digital certification infrastructure," Proceedings. Ninth IEEE International Conference on Networks, ICON 2001., Bangkok, 2001, pp. 234-239.