Design of Automated Authentication for Accessing Graded Medical Information Based on Patient Situations

Su Chong Joo

Dept. of Computer Engineering, Wonkwang University 460 Iksandaero Iksan South Korea
Tel) 82-63-850-6750, e-mail) scjoo@wku.ac.kr

1. Introduction

– The purpose of this study is to design the accessing services of the medical information via automated authentication for medical staff in consideration of dynamic situations, like emergency, of patients in the u-Medical Information System. In this paper, we suggest an automatic authentication mechanism to provide a transparent access to the medical information graded depending on normal and emergency conditions of patients. We describe how authenticated medical staff can access to the IoT-medical situation information that is obtained real-timely from biosensors and medical devices installed in the ward, and the graded patient information that is stored in a medical information server using authenticated mobile devices.

2. Design (Design of Automatic Authentication Procedures and Medical Information Service in u-Medical Information System)

- The suggested authentication procedures to be applied to the u-medical information system environment consisted of 3 Parts are shown in Image 1 in details. Authentication procedures among 3 Parts are divided into User and Mobile Device Authication phases. Especially, the Mobile Device Authentication phase is automatically exectuted unlike users(medical staff) authentication phase.

3. Results and Discussion

- In the user authentication procedures, the authentication server compares the authentication characters with user's ID/PWD respectively received from a mobile device and a medical information server, and then authenticates whether user(ex,the medical staff) is the person who is in charge of the patient or not.

The mobile device authentication procedures is executed between the mobile devices and the authentication server. The detailed procedures compare the values of the three attributes(Role, Working_Hour, Work-Location) inserted in Medical Staff Table in medical information DB with the values for the user's role, current time and the current location of mobile device, respectively.

If a patient's emergency condition and three attributes(role, working hours, current location of a mobile device)'s conditions are true entirely, it is possible to adopt to the automatic authentication. Otherwise,this mobile device authentication procedure is reqired the manual process by a user, like medical staff.

4. Conclusions

- By designing to be suitable to the purpose of the study, we plan to carry out future researches as follows; the implementation of automatic authentication on intergating a user and user's mobile devices authenications, the contruction of medical information DB graded according to the medical classification policies, and the development of a medical information access service reflected with researches mentioned above.

5. References

[1] Ghazli Abdelkader, Hadj Said Naima, and Ali Pacha Adda, "Secure Authentication Approach Based New Mobility Management Schemes for Mobile Communication", J. Inf Process Syst, Vol.13, No.1, pp.152~173, Feb. 2017.

[2] Simon S. Woo, Zuyao Li, Jelena Mirkovic, " Good Automatic Authentication Question Generation", Proceedings of The 9th INLG Conference, Edinburgh, UK, pp. 203-206, September 5-8, 2016.

[3] Su-Chong Joo, Automatic Authentication method Based on Dynamic Context for Trasparent Acees for Medical Information, Patent application in R.O.K.(10-2018-0029551), March 14, 2018.