Abstract

The Telecare Medicine Information System (TMIS) has established a connection between patients at home and doctors at a clinical center by using telecommunication systems and physiological monitoring devices. Authentication, security, patient's privacy protection and data confidentiality are important for patient or doctors accessing to Electronic Medical Records (EMR). Remote user authentication is desirable for TMIS to verify the correctness of communicating parties. The password based authentication schemes provide efficient and scalable solutions for remote user authentication. In this context, numerous schemes have been proposed to achieve these goals. However, these schemes are vulnerable to various attacks. Moreover, they are neither efficient nor user friendly. Specially, some schemes require the exponential computation or public key cryptography which leads to very low efficiency for smart card. This paper shows that recently proposed Zhian Zhu’s scheme is incorrect. Moreover, it has insecure change of password, and no early wrong password detection and session key generation. To remedy, robust authentication scheme for TMIS has been proposed using one way hash function.
References

1. Adamsk, T., Winiecki, W., Entity identification algorithms for distributed measurement and control systems with asymmetry of computational power, Prz Elektrotechniczny, (2008), No. 05
3. Pejaš, J., El Fray, I., Ruciński, A., Authentication protocol for software and hardware components in distributed electronic signature creation system, Prz Elektrotechniczny, (2012), No. 10b

Index Terms

Computer Science

Applied Sciences

Keywords

Authentication, Hash function, Password, Smart card, TMIS.