




Chapter 2

Forward and Backward Key Secrecy Preservation Scheme for Medical Internet of Things



Vincent Omollo Nyangaresi , Zaid Ameen Abduljabbar ,
Keyan Abdul-Aziz Mutlaq , Mohammed Abdulridha Hussain ,
and Zaid Alaa Hussien 

Abstract Wireless healthcare networks facilitate real-time patient monitoring and permit timely intervention when required. In so doing, they reduce healthcare costs as well enhancing the quality of patient lives. However, sensitive and private patient data is exchanged over wireless public channels. As such, numerous attacks can be launched against the collected data, violating patient privacy and causing inappropriate response from the side of the medical health workers. Although a plethora of security and privacy protocols has been developed, the extremely low computation, communication, and storage capability of the nano-sensors present some challenges in the design of robust and yet efficient security protocols. In this paper, an authentication scheme is developed that is demonstrated to provide strong mutual authentication, backward secrecy, session key negotiation, and forward key secrecy. In addition, it is shown to be resilient against numerous attacks as well as exhibiting low computation and communication complexities compared with other schemes.

V. O. Nyangaresi

Faculty of Biological and Physical Sciences, Tom Mboya University, Homabay, Kenya
e-mail: vnyangaresi@tmuc.ac.ke

Z. A. Abduljabbar (✉) · M. A. Hussain

Department of Computer Science, College of Education for Pure Sciences, University of Basrah,
Basrah 61004, Iraq
e-mail: zaid.ameen@uobasrah.edu.iq

M. A. Hussain

e-mail: mohammed.abdulridha@uobasrah.edu.iq

K. A.-A. Mutlaq

IT and Communications Center, University of Basrah, Basrah 61004, Iraq
e-mail: keyan.alsibahi@uobasrah.edu.iq; keyan.alsibahi@student.usm.my

School of Computer Sciences, Universiti Sains Malaysia, USM, Pulau Pinang, 11800 Gelugor,
Malaysia

Z. A. Hussien

Information Technology Department, Management Technical College, Southern Technical
University, Basrah, Iraq
e-mail: zaid.alaa@stu.edu.iq