Proposing Secure and Lightweight Authentication Scheme for IoT Based E-Health Applications

Maria Almulhim, Noor Zaman

College of Computer Sciences and IT, King Faisal University, Saudi Arabia

maria.almulhim1@gmail.com, nzaman@kfu.edu.sa

Abstract— **The Internet of Things (IoT) is the collection of connected smart devices\objects through internet network. The rapid development of IoT and vast expansion of wireless technologies unfold the new chances of growth in several domains such as, Education, Transportation, Agriculture, and especially in the Healthcare sector. Introducing the IoT through healthcare applications fetch several benefits, including cost savings through lowered hospital visiting costs, health care provider costs, transportation costs, human resource costs and the insurance costs. It leads to an added advantage of improved quality care in health care. However, increasing use of the IoT services in E-health applications has led to increase the concerns of security and privacy, especially in healthcare domain. In fact, healthcare applications are prone to data breaches and widening issues in security aspects owing to increasing number of access points to sensitive data through electronic medical records, as well as the rising popularity of wearable technology. For example, of these issues, authentication of the different connected entities, energy efficiency and exchanged data confidentiality form the major concerns for users. Therefore, the successful deployment of IoT-based E-health application rely on overcome the major security concerns for the users which needs to be addressed in energy efficient way. Though a number of researches have conducted for lightweight secure authentication, there is still a great room for further research to address security challenges as well as its energy efficiency for those security authentication schemes in IoT. There is a great need to design and develop a lightweight secure authentication model, which offers significant security level against multiple attacks such as mainly: Impersonation attacks, man in the middle attack and unknown key sharing attacks for IoT base E-health domain. This research proposed a secure group-based lightweight authentication scheme for IoT based E-health applications, the proposed model will provide mutual authentication and energy efficient, and computation for healthcare IoT based applications. Which will use elliptic curve cryptography (ECC) principles that provide mentioned featured of suggested model.**

Keywords— *Secure, Authentication, Light weight, ECC, IoT*

Maria Almulhim received the B.A. degree in Computer science from the College of Computer Science and Information Technology for girl in Hofuf, King Faisal University in 2012. Currently, study Master in computer science at the College of Computer Science and Information Technology, King Faisal University, Saudi Arabia. Current job, work as Application Analysis in National Guard and health affairs in Hofuf, Saudi Arabia. Her areas of interest include Software Engineering, Mobile Application Programming, Web Development, and Network Management.

Dr. Noor Zaman acquired his degree in Engineering in 1998, and Master's in Computer Sciences at the University of Agriculture at Faisalabad in 2000. His academic achievements further extended with PhD in Information Technology at University Technology Petronas (UTP) Malaysia. He has vast experience of 17 years in the field of teaching and research. He is currently working as an A. Professor at College of Computer Sciences and Information Technology, King Faisal University, Saudi Arabia since 2008. He has contributed well in King Faisal University for achieving ABET Accreditation twice, by working as an active member and Coordinator for Accreditation and Quality cell for more than 09 years. He takes care of versatile operations including teaching, research activities, leading ERP projects, IT consultancy and IT management. He headed the department of IT, and administered the prometric center in the ILMA University formerly Institute of Business and Technology (BIZTEK), in Karachi Pakistan. He has worked as a consultant for Network and Server Management remotely in Apex Canada USA base Software house and call center. Dr. Noor Zaman has authored several research papers in indexed journals\international conferences, and edited seven international reputed Computer Science area books, has many publications to his credit. He is an associate Editor, Regional Editor, Program Committee, Keynote Speaker and reviewer for reputed international journals and conferences around the world. He has completed several international research grants funded by different bodies and currently involved in different courtiers for research grants. His areas of interest include Wireless Sensor Network (WSN), Internet of Things IoT, Security, Mobile Application, Ad hoc Networks, Cloud Computing, Big Data, Mobile Computing, and Communication and Software Engineering.