جامعة الإسكندرية
ALEXANDRIA
UNIVERSITY

Faculty of Engineering
Department of Electrical Engineering

An Authentication Protocol for the Medical Internet of Things

A Thesis submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy

In

Electrical Engineering

Presented by

Nagwa Mohamed EL Meniawy

B.Sc. in Electrical Engineering,
Faculty of Engineering, Alexandria University, 2008

M.Sc. in Electrical Engineering,
Faculty of Engineering, Alexandria University, 2015

2022

ABSTRACT

The progress in biomedical sensors, Internet of Things technologies, big data, cloud computing and artificial intelligence is leading the development of e-health medical systems offering a range of new and innovative services. One such service is remote patient monitoring where medical professionals are able to collect and examine a patient's medical data remotely. Of course, in these systems, security and privacy are of utmost importance and verify the identities of system users before granting them access to sensitive patient-related data. To this end, a number of authentication protocols have been recently designed specifically for e-health systems.

Moreover, proposed protocol is an authentication protocol that enables a medical professional and the network of sensors used by a patient to authenticate each other and share a cryptographic key to be used for security in a communication session. The protocol also enables the dynamic assignment of patients to doctors in order to control access to patients' data.

A security analysis is performed of the protocol both formally, using the ProVerif protocol analysis tool, and informally demonstrating its security features. The proposed protocol shows that it achieves mutual authentication, secret key establishment, forward secrecy, and anonymity. In terms of performance, the protocol is computationally lightweight as it relies on symmetric key cryptography. This is demonstrated, by comparing the computational cost of our protocol (in terms of execution time) with that of other similar protocols.