شبكة المعلومات الجامعية

التوثيق الإلكتروني والميكروفيلم

بسم الله الرحمن الرحيم

HANAA ALY

شبكة المعلومات الجامعية

التوثيق الالكتروني والميكروفيلم

HANAA ALY

شبكة المعلومات الجامعية

التوثيق الإلكتروني والميكروفيلم

جامعة عين شمس

التوثيق الإلكتروني والميكروفيلم

قسم

نقسم بالله العظيم أن المادة التي تم توثيقها وتسجيلها
علي هذه الأقراص المدمجة قد أعدت دون أية تغيرات

يجب أن

تحفظ هذه الأقراص المدمجة بعيدا عن الغبار

HANAA ALY

Ain Shams University
Faculty of Engineering
Computer and Systems Engineering Department

A Secure Protocol for Data Exchange in the Internet of Things

A Thesis
Submitted in Partial Fulfillment of the Requirements
For the Degree of Doctor of Philosophy in Electrical Engineering
(Computer and Systems Engineering)

Submitted by
Eman Mohamed Abdel Wahab Elemam
Master of Science in Electronic Engineering
(Computer Sciences and Engineering)
Faculty of Engineering, Menoufia University,
2011

Supervised by
Prof. Dr. Ayman Mohamed Bahaa-ElDin
Dr. Mohammed Ali Sobh
Dr. Nabil Hamdy Shaker

Cairo – Egypt
2021

Ain Shams University
Faculty of Engineering
Computer and Systems Engineering Department

Approval Sheet

Name: Eman Mohamed Abdel Wahab Elemam

Thesis: A Secure Protocol for Data Exchange in the Internet of Things

Degree: Doctor of Philosophy in Electrical Engineering
(Computer and Systems Engineering)

Examiners' Committee

Name and Affiliation	Signature
1- Prof. Khaled Hussien Moustafa Vice Dean of Research and Postgraduate Professor of Computer Engineering Faculty of Computer Sciences – Misr Internationnal University **(Examiner)**	…….
2- Prof. Mohamed Mahmoud Taher Computers and Systems Engineering Department Faculty of Engineering – Ain Shams University **(Examiner)**	…….
3- Prof. Dr. Ayman Mohamed Bahaa-ElDin Computers and Systems Engineering Department Faculty of Engineering – Ain Shams University **(Supervisor)**	…….
4- Dr. Mohammed Ali Sobh Computers and Systems Engineering Department Faculty of Engineering – Ain Shams University **(Supervisor)**	…….

Examination Date: .../... /……

Statement

This thesis is submitted to Ain Shams University in partial fulfilment of the requirements for the degree of Doctor of Philosophy in Electrical Engineering (Computer and Systems Engineering).

The work included in this thesis was carried out by the author at Computer and Systems Engineering Department, Faculty of Engineering, Ain Shams University.

No part of this thesis has been submitted for a degree or a qualification at any other scientific entity.

Eman Mohamed Abdel Wahab Elemam
Computer and Systems Engineering Department
Faculty of Engineering
Ain Shams University
Cairo, Egypt
2021

Signature
……...…….
Date: … / … / ……

Researcher Data

Name: Eman Mohamed Abdel Wahab Elemam

Date of birth: 26/11/1977

Place of birth: Cairo

Last academic degree: Master of Science

Field of specialization: Electronic Engineering
(Computer Science and Engineering)

University issued the degree: Menoufia University

Date of issued degree: 2011

Thesis Abstract

Eman Mohamed Abdel Wahab Elemam

A Secure Protocol for Data Exchange in the Internet of Things

Doctor of Philosophy in Electrical Engineering
(Computer and Systems Engineering)

Ain Shams University, 2021

This thesis contributes to the body of knowledge in the area of security protocols for IoT networks as there is no security standardization that governs the implementations of these platforms. Also, the usage of IoT technology to combat COVID-19 pandemic boosts IoT market especially in the healthcare sector. Thus, the security and the privacy for the patients data is highly important where if it is forged before reaching to doctors, wrong diagnosing may threaten the precious patients' lives and also may threaten those who are surrounding them.

MQTT (Message Queue Telemetry Transport) protocol is widely used as an application layer protocol in IoT environment and the current MQTT standard does not specify how MQTT can provide cryptographic services like authentication, access control, confidentiality, etc. that maintain the MQTT based IoT system secure. Thus, PMQTT (Protected MQTT) protocol is introduced in this thesis to keep MQTT systems secure. A Telemedicine case study was selected to clarify the proposed security protocol.

PMQTT design has three cryptographic stages. The first stage is the authentication stage and it is based on ECDSA. The second phase is the key establishment and distribution phase and it is using ECDH to generate shared key between the two communicating parties through PMQTT Broker. The last phase is the confidentiality phase and it is based on AES 128 using the generated shared key of the previous phase.

Then, formal verification for PMQTT is conducted using ProVerif 2.00 cryptographic protocol verifier tool. It was found that the queries regarding the client's authenticity and the secrecy of both the session key and the encrypted messages are proven to be true.

After that, performance analysis of PMQTT is conducted using practical implementation with MPIR 3.0.0 big integers' library on Visual Studio 2017 and the domain parameters of secp256k1 elliptic curve in conjunction with biomedical data set from PhysioNet database. Afterwards, performance metrics are measured for the security phases of PMQTT by taking the mean of 50 trials from the execution of the testing scenario. Finally, a comparison between PMQTT performance metrics and previous work is conducted. It was concluded that PMQTT offers the required security services with satisfying performance capabilities.

Keywords:

Internet of Things (IoT), Authentication, Confidentiality, Message Queue Telemetry Transport (MQTT), Elliptic Curve Digital Signature Algorithm (ECDSA), Elliptic Curve Diffie Helman (ECDH), Advanced Encryption Standard (AES), Elliptic Curve Diffie Hellman, Formal verification, ProVerif.

Acknowledgment

The whole gratitude is due to ALLAH. I would like to express my profound gratitude to Prof. Ayman Bahaa-ElDin for his great efforts in this study. Thanks to his insightful remarks, and limitless generosity with guidance and support. Also, I wish to express my deep appreciation to Assoc. Prof. Mohamed Sobh for his valuable suggestions. I must thank Dr. Nabil Hamdy for his enthusiastic supervision, valuable ideas, and his incessant follow-up of the minute's details. My deep appreciation must go to the examiners committee for their great efforts and support.

Last but not least, I would like to express my profound gratitude to my family; my parents, my husband, my daughters, and my brothers for their continuous encouragement, patience, care and support in my all life.