UTS UNIVERSITY OF TECHNOLOGY SYDNEY

[Security and Privacy Preserving Schemes in Smart Homes using Blockchain]

by [Amjad Mohammed Qashlan]

Thesis submitted in fulfilment of the requirements for the degree of

[Doctor of Philosophy]

under the supervision of [**Dr. Priyadarsi Nanda (Principle supervisor)**
Dr. Manoranjan Mohanty (Co-supervisor)]

University of Technology Sydney
Faculty of [Engineering and Information Technology]

[November 2021]

CERTIFICATE OF ORIGINAL AUTHORSHIP

I, *Amjad Qashlan* declare that this thesis, is submitted in fulfilment of the requirements for the award of *Doctor of Philosophy* in the *School of Electrical and Data Engineering /Faculty of Engineering and Information Technology*, at the University of Technology Sydney.

This thesis is wholly my own work unless otherwise referenced or acknowledged. In addition, I certify that all information sources and literature used are indicated in the thesis.

This document has not been submitted for qualifications at any other academic institution.

This research is supported by the Australian Government Research Training Program.

SIGNATURE: _____

[Amjad Qashlan]

DATE: 30th November, 2021

Abstract

Emerging technologies such as the Internet of Things, sensors, and communication networks have been integrated into traditional homes to provide a wide range of smart home services to simplify and improve people‚Äôs lifestyles. However, as the Internet of Things has grown in popularity, so have the concerns it poses. As a result, concerns like data privacy, security, and decentralisation of IoT systems present substantial threats to the future of smart home IoTs.

This thesis presents efforts towards a blockchain-based smart home framework which supports data confidentiality, differential privacy, and robustness. The thesis achieves three novel contributions. We first deploy a private blockchain using Ethereum smart contracts for a smart home to ensure only the homeowner can access and monitor home appliances. The smart contracts are designed to allow devices to communicate without the need for a trusted third party. Our prototype demonstrates three key elements of blockchain-based smart security solutions for smart home applications: smart contracts, blockchain-based access control, and the performance evaluation of the proposed scheme.

Next, we propose an authentication scheme that integrates attribute-based access control using smart contracts with an ERC-20 Token (Ethereum Request For Comments) and edge computing to construct a secure framework for IoT devices in a smart home system. The edge server provides scalability to the system by offloading heavier computation tasks to edge servers. We present the system architecture and design and discuss various aspects of testing and implementing smart contracts.

Finally, we conduct a performance evaluation to demonstrate the feasibility and efficiency of the proposed scheme. The core features that blockchain technology is leveraged upon are a trust-less environment, immutability and transparency, which come at the cost of a lack of data privacy. Therefore, we propose a privacy-preserving architecture for smart home-based blockchain. The architecture utilises differential privacy machine learning algorithm to send private IoT smart home data to the cloud and achieve data privacy. The main objective of the model is to protect privacy with high accuracy when aggregating the data from traffic analysis, linking and mining attacks by adding Gaussian noise. The implementation of our model ensures better accuracy and improved model utility. The goal of the privacy protection scheme used in our architecture is to enable smart home data to be used without disclosing privacy and provide published data to different service providers with lower information loss and higher data utility.

Dedication

To my honorable parents (Mohammed & Mona), my soulmate (Hesham) my lovely little angels (Saja, Yosif, Salem and Moaaz)
and to the memory of my Father-in-law (Salem), I wish we were around in your last days.
. . .

ACKNOWLEDGMENTS

Firstly, I would like to express my sincere gratitude to Almighty God for guiding me and blessing me with physical and mental strength along this PhD journey.

I would like to express my sincere gratitude to my supervisor, Dr. Priyadarsi Nanda, whose expertise, understanding, and patience added considerably to my graduate experience. I am greatly thankful for his continuous encouragement that guided me throughout this journey of becoming a successful researcher. Dr. Nanda's guidance, patience, and continuous support were essential to the completion of this thesis. His knowledge and invaluable feedback immensely helped me go forward in my research. I am greatly indebted to him for helping me get through the challenging times. I would like to thank my Co-supervisor, Dr. Manoranjan Mohanty, who provided valuable and expert feedback on my work. His support, co-operation, and generosity throughout the research tenure are truly undeniable.

This research would not have been possible without the support from my family. I would like to thank my parents, Mohammed and Mona, for motivating and encouraging me to be the best. Thanks for all your prayers that enlightened my journey and kept me going. Special thanks to my kids, Saja, Yosif, Salem and Moaaz, for the numerous sacrifices, continuous support, endless love and all the sorry cards that melted my heart. Many thanks to my husband, Hesham, for sharing my dream and making it come true together and for all the effort he put in to make me realise how strong and independent I am.

I would like to extend my gratitude to my sisters, Baraa and Eman, for their love, support and care all the time and, of course, many thanks to all my brothers; Bandar, Amjed, Ahmad, Ayman, Osama.

A big thanks to all my friends (Hana, Maha, Abrar, Abeer, Amani, Enaam, Maryam, Wafaa, Aisha) for sharing PhD advice, parental tips and being my sisters in foreign land. I also wish to thank all my colleagues from the School of Electrical and Data Engineering at the University of Technology Sydney. Specifically, I would like to thank Annie, Ambar, Nisha and Upasana for creating a friendly atmosphere in the group and assisting me in whatever manner possible.

Although this journey got harder and harder as I cried in frustration or got some sleepless nights, it taught me that there will always be light at the end of the tunnel.

List of Publications

Journal Papers :

1. **A. Qashlan**, P. Nanda, X. He, and M. Mohanty, Privacy-preserving mecha-nism in smart home using blockchain, IEEE Access 9 (2021) 103651-103669. **Impact factor of 3.367**

2. **A. Qashlan**, P. Nanda, and M. Mohanty, Differential Privacy Model for Blockchain based Smart Home Architecture, Submitted to Future Generation Computer Systems Journal (FGCS), Under review, **Impact factor of 7.187**

Conference Papers

1. **A. Qashlan**, P. Nanda, and X. He, "Security and privacy implementation in smart home: Attributes based access control and smart contracts," in 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). IEEE, pp. 951- 958. **(Rank A)**

2. **A. Qashlan**, P. Nanda, and X. He, "Automated Ethereum smart contract for blockchain based smart home security", in Smart Systems and IoT: Innovations in Computing, Springer, 2020, pp. 313-326

TABLE OF CONTENTS

List of Figures

List of Tables