DECENTRALISED ACCESS CONTROL FRAMEWORK FOR IOT SECURITY BY LEVERAGING BLOCKCHAIN TECHNOLOGY IN SMART FARMING

NORMAIZEERAH BINTI MOHD NOOR

DOCTOR OF PHILOSOPHY
(COMPUTER SCIENCE)

UNIVERSITI PERTAHANAN NASIONAL MALAYSIA

2023

DECENTRALISED ACCESS CONTROL FRAMEWORK FOR IOT SECURITY BY LEVERAGING BLOCKCHAIN TECHNOLOGY IN SMART FARMING.

NORMAIZEERAH BINTI MOHD NOOR

Thesis submitted to the Centre for Graduate Studies, Universiti Pertahanan Nasional Malaysia, in fulfilment of the requirements for the Degree of Doctor of Philosophy (Computer Science)

2023

ABSTRACT

Integrating the Internet of Things (IoT) in smart farming has led to significant advancements in agricultural ecosystems. Smart farming aims to enhance performance and production quality by automating various processes. However, the rapid adoption of IoT in smart farming has introduced cybersecurity threats, particularly related to access control. Existing access control models in IoT, Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role-Based Access Control (RBAC), Attributed-Based Access Control (ABAC) Organisation-Based Access Control (OrBAC), Usage-Based Access Control (UCON), Capability-Based Access Control (CapBAC), and Hybrid-Based Access Control (HBAC), are common centralized and face challenges in scalability and efficiency within IoT ecosystems. Thus, in this study proposed framework adapting blockchain technology to create a secure and decentralised approach for securing and protecting IoT devices from unauthorised access by anomalous entities. The framework is built upon a four-layer architecture by adapting the FRABAC model, a combination of RBAC and ABAC to develop fine-grained access control policies that are enforced through smart contracts on the blockchain. The research demonstrates the effectiveness and validation of the decentralised access control mechanism through simulation experiments and blockchain performance metrics evaluation. The evaluation results highlight that the proposed framework demonstrates low-cost consumption when paying transaction fees for executing the smart contracts of IoT_SRMC, IoT_ORMC, and IoT_ACC.

Additionally, the evaluation reveals that the addDevice() and addResource() operations experienced slightly higher latencies of 363161ms and 367382ms, respectively, in the case of 150 requested transactions. In contrast, the addTypeRLItem() operation demonstrated a lower latency of 905ms in 150 transaction requests compared to the addDevice() and addResource() operations. While the transaction throughput of addDevice(), addTypeRLItem() operations has reveal high transaction throughput of 75 tps at 150 requested transaction, and addResource() operations has reveal slightly low transaction throughput of 37.5 tps at 150. Thus, the findings in this study have the potential to address scalability, heterogeneity, low-cost consumption, and resource constraints related to IoT devices and applicable to apply in smart farming practices. Additionally, it serves as a foundation for formatting access policies in multiple entities and heterogeneous IoT environments across any IoT domain, requiring specific justifications for identification. The study establishes a basis for future advances in ensuring secure access to IoT devices and resources across diverse domains and opens new opportunities for researchers to apply decentralised access control for the IoT environment.

ABSTRAK

Internet Benda (IoT) dalam pertanian pintar telah membawa kemajuan yang signifikan dalam ekosistem pertanian. Pertanian pintar bertujuan untuk meningkatkan prestasi dan kualiti pengeluaran dengan mengautomasikan pelbagai proses. Walau bagaimanapun, penggunaan pantas IoT dalam pertanian pintar telah memperkenalkan ancaman keselamatan siber, terutamanya berkaitan dengan kawalan akses. Model kawalan capaian sedia ada dalam IoT, Kawalan Capaian Budi Bicara (DAC), Kawalan Capaian Mandatori (MAC), Kawalan Akses Berasaskan Peranan (RBAC), Kawalan Akses Berasaskan Atribut (ABAC) Kawalan Akses Berasaskan Organisasi (OrBAC), Berasaskan Penggunaan Kawalan Capaian (UCON), Kawalan Capaian Berasaskan Keupayaan (CapBAC) dan Kawalan Akses Berasaskan Hibrid (HBAC), adalah berpusat biasa dan menghadapi cabaran dalam skalabiliti dan kecekapan dalam ekosistem IoT. Oleh itu, dalam kajian ini mencadangkan rangka kerja menyesuaikan teknologi blockchain untuk mencipta pendekatan yang selamat dan desentralisasi untuk mengamankan dan melindungi peranti IoT daripada akses tanpa kebenaran oleh entiti anomali. Kerangka ini dibina berdasarkan senibina empat lapisan dan menggunakan model FRABAC, gabungan Kawalan Akses Berasaskan Peranan (RBAC) dan Kawalan Akses Berasaskan Atribut (ABAC), untuk membangunkan dasar kawalan akses bergranulasi halus yang dilaksanakan melalui kontrak pintar di blockchain. Penyelidikan ini menunjukkan keberkesanan dan pengesahan mekanisme

kawalan akses terdesentralisasi melalui eksperimen simulasi dan penilaian metrik prestasi blockchain. Keputusan penilaian menyerlahkan bahawa rangka kerja yang dicadangkan menunjukkan penggunaan kos rendah apabila membayar yuran transaksi untuk melaksanakan kontrak pintar IoT_SRMC, IoT_ORMC dan IoT_ACC. Selain itu, penilaian mendedahkan bahawa operasi addDevice() dan addResource() mengalami latensi yang lebih tinggi sedikit sebanyak 363161ms dan 367382ms, masing-masing, dalam kes 150 transaksi yang diminta. Sebaliknya, operasi addTypeRLItem() menunjukkan daya pengeluaran transaksi yang lebih rendah sebanyak 905ms dalam 150 permintaan transaksi berbanding dengan operasi addDevice() dan addResource().Sementara itu, operasi urus niaga addDevice(), addTypeRLItem() telah mendedahkan daya urus niaga yang tinggi sebanyak 75 tps pada 150 transaksi yang diminta, dan operasi addResource() telah mendedahkan daya urus niaga yang rendah sedikit sebanyak 37.5 tps pada 150. Oleh itu, penemuan dalam kajian ini berpotensi untuk menangani skalabiliti, heterogeniti, penggunaan tenaga yang tinggi, dan kekangan sumber yang berkaitan dengan peranti IoT dan boleh digunakan dalam amalan pertanian pintar.Ini menunjukkan bahawa kerangka yang dicadangkan boleh digunakan dengan berkesan dalam amalan pertanian pintar kerana keberkesanan kos dan prestasi yang lebih baik. Selain itu, ia berfungsi sebagai asas untuk membangunkan dasar akses dalam berbilang entiti dan persekitaran IoT heterogen yang boleh dipraktikan di lain-lain bidang IoT, yang memerlukan justifikasi khusus untuk pengenalpastian. Kajian itu mewujudkan asas untuk kemajuan masa depan dalam memastikan akses selamat kepada peranti dan sumber IoT merentasi pelbagai bidang dan membuka peluang baharu kepada penyelidik untuk menggunakan kawalan akses desentralisasi di persekitaran IoT.

ACKNOWLEDGEMENTS

I would like to express my deepest thankfulness to my main supervisor, Prof Madya Ts. Dr. Afiza, for her genuine passion for research and teaching, invaluable guidance, wisdom, and remarkable patience throughout every step of my academic journey. Her unwavering dedication and kind support have been instrumental in keeping me motivated and on the right path, ultimately leading to the successful completion of this study. I am truly grateful to my co-supervisors Ts. Dr. Asiakin for generously sharing their knowledge and providing valuable advice to enhance my research. I express my special appreciation to Dr Muslihah and Mister Khairul Khalil for their invaluable views and sharing on the access control mechanism and blockchain opinions. I am also thankful to the examiners for their comments and suggestions, which have significantly contributed to the improvement of this thesis.

Numerous organizations and individuals have provided support during my study, and I sincerely wish to thank CGS and FSTP UPNM for their valuable assistance throughout the process. Additionally, I am fortunate to have had supportive and understanding colleagues and friends during my academic journey, especially Miss Atiqah and Puan Nuraini, who guided me towards my main supervisor.

I extend my heartfelt appreciation to my husband, Muhamad Azwan, for his unwavering support and attention, enabling me to complete my dissertation. I am also grateful to my family for their sincere prayers, love, and immense inspiration, which

have been instrumental in motivating me during my PhD studies. The dedication and sacrifices of my husband and parents have given me the strength and inspiration to pursue my goals. Thank you from the bottom of my heart.

I look forward excited about embarking on more adventures and exploring knowledge that not only benefits us but also the people around us, bringing us closer to Allah. Insya-Allah, may we continue this journey of learning and growth together.

APPROVAL

The Examination Committee has met on **20 October 2023** to conduct the final examination of **Normaizeerah Binti Mohd Noor** on his degree thesis entitled **Decentralised Access Control Framework for IoT Security by Leveraging Blockchain Technology in Smart Farming.**

The committee recommends that the student be awarded the of Doctor of Philosophy (Computer Science).

Members of the Examination Committee were as follows.

Prof. Ts. Gs. Dr. Mohd 'Afizi bin Mohd Shukran
Faculty of Defence Science and Technology
Universiti Pertahanan Nasional Malaysia
(Chairman)

Prof. Dr. Mohd Nazri bin Ismail
Faculty of Defence Science and Technology
Universiti Pertahanan Nasional Malaysia
(Internal Examiner)

Prof. Madya Dr. Chiew Kang Leng
Research and Commercialization
Universiti Malaysia Sarawak
(External Examiner)

Prof. Madya Ts. Dr. Nik Zulkarnaen Khidzi
Faculty of Creative Technology and Heritage
Universiti Malaysia Kelatan
(External Examiner)

APPROVAL

This thesis was submitted to the Senate of Universiti Pertahanan Nasional Malaysia and has been accepted as fulfilment of the requirements for the degree of **Doctor of Philosophy (Computer Science)**. The members of the Supervisory Committee were as follows.

Noor Afiza binti Mat Razali, PhD
Prof. Madya Ts.
Faculty of Defence Science and Technology
Universiti Pertahanan Nasional Malaysia
(Main Supervisor)

Nor Asiakin binti Hasbullah, PhD
Ts.
Faculty of Defence Science and Technology
Universiti Pertahanan Nasional Malaysia
(Co-Supervisor)

Muslihah binti Wook, PhD
Faculty of Defence Science and Technology
Universiti Pertahanan Nasional Malaysia
(Co-Supervisor)

UNIVERSITI PERTAHANAN NASIONAL MALAYSIA

DECLARATION OF THESIS

Student's full name : Normaizeerah Binti Mohd Noor

Date of birth : 13 April 1998

Title : Decentralised Access Control Framework for IoT Security by Leveraging Blockchain Technology in Smart Farming.

Academic session : 2021/2022

I hereby declare that the work in this thesis is my own except for quotations and summaries which have been duly acknowledged.

I further declare that this thesis is classified as:

☐ **CONFIDENTIAL** (Contains confidential information under the official Secret Act 1972)*

☐ **RESTRICTED** (Contains restricted information as specified by the organisation where research was done)*

☒ **OPEN ACCESS** I agree that my thesis to be published as online open access (full text)

I acknowledge that Universiti Pertahanan Nasional Malaysia reserves the right as follows.

1. The thesis is the property of Universiti Pertahanan Nasional Malaysia.
2. The library of Universiti Pertahanan Nasional Malaysia has the right to make copies for the purpose of research only.
3. The library has the right to make copies of the thesis for academic exchange.

_____	_____
Signature	**Signature of Supervisor/Dean of CGS/ Chief Librarian
_____	_____
IC/Passport No.	**Name of Supervisor/Dean of CGS/ Chief Librarian
Date:	Date:

*If the thesis is CONFIDENTAL OR RESTRICTED, please attach the letter from the organisation with period and reasons for confidentiality and restriction.

** Witness

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

IoT	-	Internet of Things
UN	-	United Nations
UAV	-	Unmanned Aerial Vehicles
DAC	-	Discretionary Access Control
MAC	-	Mandatory Access Control
RBAC	-	Role-Based Access Control
OrBAC	-	Organisation-Based Access Control
UCON	-	Usage-Based Access Control
CapBAC	-	Capability-Based Access Control
HBAC	-	Hybrid-Based Access Control
PoW	-	Proof of Work
PoS	-	Proof of Stake
PBFT	-	Practical Byzantine Fault Tolerance
FRABAC	-	Fine-Grained Role-Attribute Access Control
PERBAC	-	Pervasive-Based Access Control
ABAC	-	Attribute-Base Access Control
RQ	-	Research Questions

RO	-	Research Objectives
EO	-	Expected Outcome
RFID	-	Radio Frequency Identification
LAN	-	Local Area Network
PAN	-	Personal Area Network
WAN	-	Wide Area Network
GSM	-	Global System for Mobile communication
IP	-	Internet Protocol
HTTP	-	Hypertext Transfer Protocol
CoAP	-	Constrained Application Protocol
MQTT	-	Message Queue Telemetry Transport
DOS	-	Disk Operating System
DDOS	-	Distributed Denial-Of-Service
ID	-	Identification
XSS	-	Cross-Site Scripting
CSRF	-	Cross-Site Request Forgery
SQL	-	Structured Query Language
RF	-	Radio Frequency
UPnP	-	Universal Plug-and-Play
MITM	-	Man-In-The-Middle
RPL	-	Recognition of Prior Learning
WSN	-	Wireless Sensor Networks
TCP	-	Transmission Control Protocol

UDP	-	User Datagram Protocol
XML	-	Extensible Markup Language
XXE	-	External Entity Injection
LDAP	-	Lightweight Directory Access Protocol
ICMP	-	Internet Control Message Protocol
CPU	-	Central Processing Unit
API	-	Application Programming Interface
AC	-	Access Control
ACLs	-	Access Control Lists
XACML	-	Extensible Access Control Markup Language
AWS	-	Amazon Web Services
TRABAC	-	Tokenised Role-Attribute Based Access Control
UMA	-	User-Managed Access
SPV	-	Simplified Payment Verification
PoA	-	Proof-of-Authority
DApps	-	Decentralised Applications
EVM	-	Ethereum Virtual Machine
EOA	-	Externally Owned Accounts
ETH	-	Ether
PC	-	Policy Contract
SC	-	Smart Contract
TRS	-	Trust and Reputation System
IPFS	-	Interplanetary File System

ERC	-	Earnings Response Coefficient
Eos	-	Electro-Optical System
EHR	-	Electronic Health Records
BHE-AC	-	Blockchain-based high-efficiency access control framework
CAC	-	Customer Acquisition Cost
IoMT	-	Internet Of Medical Things
SRAC	-	Selective Ring-Based Access Control
PDP	-	Policy Decision Point
PAP	-	Policy Administration Point
PBFT	-	Practical Byzantine Fault Tolerance
PMC	-	Policy Management Contract
SAMC	-	Subject Attribute Management Contract
OAMC	-	Object Attribute Management Contract
ACC	-	Access Control Contract
ABIs	-	Application Binary Interfaces
ADAC	-	Attribute-Based Distributed Access Control
DADAC	-	Dynamic Attribute-Based Distributed Access Control
OC	-	Object Contract
SA	-	Subject Attribute
OA	-	Object Attribute
EA	-	Environment Attribute
RBAC-SC	-	Role-Based Access Control Smart Contract
DHACS	-	Decentralised Hybrid Access Control