

**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 dipraktikkan 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 Kelantan  
(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 CONFIDENTIAL OR RESTRICTED, please attach the letter from the organisation with period and reasons for confidentiality and restriction.

\*\* Witness

## TABLE OF CONTENTS

<b>ABSTRACT</b>	<b>ii</b>
<b>ABSTRAK</b>	<b>iv</b>
<b>ACKNOWLEDGEMENTS</b>	<b>vi</b>
<b>APPROVAL</b>	<b>viii</b>
<b>DECLARATION OF THESIS</b>	<b>x</b>
<b>TABLE OF CONTENTS</b>	<b>xi</b>
<b>LIST OF TABLES</b>	<b>xvi</b>
<b>LIST OF FIGURES</b>	<b>xviii</b>
<b>LIST OF ABBREVIATIONS</b>	<b>xx</b>
<b>CHAPTER 1</b>	<b>1</b>
<b>INTRODUCTION</b>	<b>1</b>
<b>1.1 CHAPTER OVERVIEW</b>	<b>3</b>
<b>1.2 BACKGROUND OF STUDY</b>	<b>4</b>
1.2.1 Introduction of Internet of Thing (IoT)	4
1.2.2 Smart Farming based on the IoT	5
1.2.3 Problem and challenges in the application of IoT	7
1.2.4 Access control in the IoT	8
1.2.5 Blockchain technology for IoT access control	10
<b>1.3 PROBLEM STATEMENTS</b>	<b>11</b>
<b>1.4 RESEARCH OBJECTIVE</b>	<b>14</b>
<b>1.5 RESEARCH QUESTIONS</b>	<b>14</b>
<b>1.6 SCOPE AND LIMITATIONS</b>	<b>16</b>
<b>1.7 RESEARCH CONTRIBUTIONS</b>	<b>16</b>
<b>1.8 THESIS STRUCTURE</b>	<b>17</b>
<b>1.9 SUMMARY</b>	<b>18</b>
<b>CHAPTER 2</b>	<b>19</b>
<b>LITERATURE REVIEW</b>	<b>19</b>
<b>2.1 CHAPTER OVERVIEW</b>	<b>19</b>
<b>2.2 IoT paradigm in smart farming</b>	<b>20</b>
<b>2.3 IoT architecture and technologies</b>	<b>22</b>
<b>2.4 Problems and challenges in application of IoT</b>	<b>27</b>
2.4.1 Problem related to the characteristics of IoT	27
2.4.2 Security threats and attacks in IoT systems	30

2.4.2.1	Attacks in the physical layer	37
2.4.2.2	Attacks in the network layer	38
2.4.2.3	Attacks in the middleware layer	39
2.4.2.4	Attacks in the application layer	40
<b>2.5</b>	<b>Access control as a countermeasure for IoT Technologies in smart farming</b>	<b>43</b>
2.5.1	Basic concept of access control	44
2.5.2	Access control models in IoT	46
2.5.2.1	Discretionary-based Access Control (DAC)	49
2.5.2.2	Mandatory-based Access Control (MAC)	50
2.5.2.3	Role-based Access Control (RBAC)	51
2.5.2.4	Organisation-based Access Control (OrBAC)	53
2.5.2.5	Attribute-based Access Control (ABAC)	55
2.5.2.6	Usage Control (UCON)	56
2.5.2.7	Capability-based Access Control (CapBAC)	58
2.5.2.8	Hybrid-based access control (HBAC)	59
2.5.3	Access control policies for IoT	64
2.5.3.1	Policy specification	62
2.5.3.2	Policy management	67
2.5.3.3	Policy evaluation	68
2.5.3.4	Policy enforcement	69
<b>2.6</b>	<b>Blockchain technology as a decentralised approach for IoT access control</b>	<b>70</b>
2.6.1	Basic concept of blockchain technology	71
2.6.1.1	Nodes	72
2.6.1.2	Blocks	74
2.6.1.3	Consensus algorithm	75
2.6.1.4	Smartcontract	77
2.6.2	Governance	79
2.6.2.1	Public (permissionless)	80
2.6.2.2	Private (permissioned)	81
2.6.2.3	Hybrid	82
2.6.2	Ethereum blockchain platform	83
2.6.3.1	Ethereum Accounts	85
2.6.3.2	Difference between transaction and messages	86
2.6.3.3	Gas	87
<b>2.7</b>	<b>Related work – IoT access control using blockchain</b>	<b>88</b>
2.7.1	Blockchain-based approaches	103
2.7.1.1	Smart contract-based access control in IoT	103
2.7.1.1	Token-based access control in IoT	107
2.7.2	Non-blockchain-based approach	109

<b>2.8</b>	<b>Evaluation of blockchain performance metrics and tools</b>	<b>110</b>
<b>2.9</b>	<b>SUMMARY</b>	<b>117</b>
<b>CHAPTER 3</b>		<b>119</b>
<b>FRAMEWORK AND METHODOLOGY</b>		<b>119</b>
<b>3.1</b>	<b>CHAPTER OVERVIEW</b>	<b>119</b>
<b>3.2</b>	<b>Proposed Theoretical Framework (Decentralised Access Control for IoT Security by leveraging Blockchain Technology in Smart Farming)</b>	<b>121</b>
<b>3.3</b>	<b>Policy Component</b>	<b>124</b>
3.3.1	Contract Owner (owner of IoT device)	124
3.3.2	IoT Heterogenous Devices (the devices want to access the resources)	125
<b>3.4</b>	<b>Proposed Framework Architeture</b>	<b>125</b>
3.4.1	Physical layer	126
3.4.2	Network layer	128
3.4.3	Transaction layer (blockchain layer)	129
3.4.4	Application layer	130
<b>3.5</b>	<b>Smart contract-based access control model</b>	<b>130</b>
3.5.1	Subject-Role Managemet Contract (IoT_SRMC)	132
3.5.2	Object-Rules Management Contract (IoT_ORMC)	133
3.5.3	Access Control Contract (IoT_ACC)	135
<b>3.6</b>	<b>Access Policy Creation Framework</b>	<b>136</b>
3.6.1	Step 1: Create policy specification and statement	137
3.6.2	Step 2: Manage access control policies	138
3.6.3	Step 3: Execute policy evaluation	140
3.6.4	Step 4: Establish policy enforcement	142
<b>3.7</b>	<b>RESARCH METHODOLOGY</b>	<b>145</b>
<b>3.8</b>	<b>RESEARCH DESIGN</b>	<b>148</b>
3.8.1	Phase 1 - Theoretical Study	150
3.8.2	Phase 2 – Theoretical Frameworks Development	150
3.8.2.1	Ethereum-based Smart Contract for Decentralised Platform	151
3.8.2.2	Hybrid Access Control Models for Access Policy and Permission	151
3.8.3	Phase 3 - Exploratory Study	152
3.8.3.1	Experimental Analysis	153
	Stage 1: Experimental setup	155

Stage 2: Smart contract deployment	158
Stage 3: Experiment execution- Implementation of access control that was presented as part of the proposed framework.	168
3.8.4 Phase 4 - Validation of Experiment Study	173
Stage 4: Evaluation of blockchain performance metric	173
3.8.4.1 Cost consumption	173
3.8.4.2 Transaction throughput	174
3.8.4.3 Transaction latency	175
<b>3.9 SUMMARY</b>	<b>176</b>
<b>CHAPTER 4</b>	<b>177</b>
<b>RESULTS AND DISCUSSION</b>	<b>177</b>
<b>4.1 CHAPTER OVERVIEW</b>	<b>177</b>
<b>4.2 Experiment Scenario</b>	<b>178</b>
4.2.1 Outcome of the experiments based on the scenario	181
<b>4.3 Result and Discussion of Blockchain Performance Metrics</b>	<b>184</b>
4.3.1 Cost consumption	184
4.3.1.1 Deployment cost consumption in proposed smart contract	184
4.3.1.2 Transaction cost consumption in proposed smart contract function	187
1) Transaction costs in managing attributes and roles of a subject.	188
2) Transaction costs in managing attributes and roles of a objects.	192
3) Transaction costs in managing access policy	195
4) Transaction costs in access policy enforcement and evaluation.	197
4.3.2 Execution time of proposed smart contract function	198
4.3.3 Transaction throughput and latency	199
4.3.4 Comparison transaction throughput and latency in Ganache local network, Goerli and Sepolia testnet network.	204
<b>4.4 SUMMARY</b>	<b>209</b>
<b>CHAPTER 5</b>	<b>211</b>
<b>CONCLUSION AND RECOMMENDATION</b>	<b>211</b>

<b>5.1</b>	<b>CHAPTER OVERVIEW</b>	<b>211</b>
<b>5.2</b>	<b>RESEARCH CRITERIA CHECKLIST</b>	<b>212</b>
<b>5.3</b>	<b>RESEARCH SUMMARY</b>	<b>215</b>
<b>5.4</b>	<b>LIMITATIONS</b>	<b>216</b>
<b>5.5</b>	<b>CHALLENGES</b>	<b>217</b>
<b>5.6</b>	<b>FUTURE RESEARCH</b>	<b>218</b>
<b>5.7</b>	<b>SUMMARY</b>	<b>221</b>
	<b>REFERENCES</b>	<b>211</b>
	<b>APPENDICES</b>	<b>234</b>
	<b>APPENDIX A: SOLIDITY CODING (BACK-END)</b>	<b>234</b>
	<b>APPENDIX B: WEB3.JS AND NODE.JS CODING (FRONT-END)</b>	<b>241</b>
	<b>APPENDIX C: DATA COLLECTION OF DEPLOYMENT COST CONSUMPTION</b>	<b>250</b>
	<b>APPENDIX D: DATA COLLECTION OF TRANSACTION COST</b>	<b>251</b>
	<b>APPENDIX E: DATA COLLECTION FROM DIFFERENT TESTNET NETWORK</b>	<b>257</b>
	<b>BIODATA OF STUDENT</b>	<b>274</b>
	<b>LIST OF PUBLICATION</b>	<b>275</b>

## LIST OF TABLES

<b>TABLE NO.</b>	<b>TITLE</b>	<b>PAGE</b>
<b>Table 1.1</b>	Alignments between RQ, RO, and EO of this research	<b>15</b>
<b>Table 2.1</b>	Common threats and attacks in different layers of IoT architectures	<b>31</b>
<b>Table 2.2</b>	A summary of access control models in IoT applications	<b>47</b>
<b>Table 2.3</b>	Summarised criteria for formulating access policies in IoT systems	<b>63</b>
<b>Table 2.4</b>	A summary of previous studies on IoT access control using blockchain according to services, governance, platform, type of transaction, access control model, type of consensus, domain, and maturity level	<b>90</b>
<b>Table 2.5</b>	Performance metrics and tools for experiment	<b>110</b>
<b>Table 3.1</b>	Type of nodes and their responsibilities	<b>127</b>
<b>Table 3.2</b>	Description of all sample access policies based on hybrid access control model	<b>144</b>
<b>Table 3.3</b>	Hardware and software specifications	<b>155</b>
<b>Table 3.4</b>	Example of access policy in IoT_ORMC	<b>160</b>
<b>Table 3.5</b>	Example of access policy in IoT_SRMC	<b>162</b>
<b>Table 4.1</b>	Device attribute information based smart farming environment.	<b>180</b>

<b>Table 4.2</b>	Creation of access policy framework	<b>181</b>
<b>Table 4.3</b>	Transaction cost and the gas used in managing attributes and roles of a subject in each function within proposed schemes.	<b>191</b>
<b>Table 4.4</b>	Transaction cost and the gas used in managing attributes and roles of objects in each function within schemes.	<b>194</b>
<b>Table 4.5</b>	Transaction cost and gas used in managing access policy	<b>196</b>
<b>Table 4.6</b>	Transaction cost, gas used and execution time in managing access control permission in each function within proposed schemes.	<b>197</b>
<b>Table 4.7</b>	The execution time, gas used, transaction cost, transaction throughput and latency for execution proposed framework scheme in different functions of contracts	<b>204</b>
<b>Table 4.8</b>	Comparison of transaction throughput, latency, and execution time in the different testnet platforms for concurrent requests (10, 50, and 100)	<b>205</b>
<b>Table 5.1</b>	Summary of the foundation of the research design	<b>213</b>

## LIST OF FIGURES

<b>FIGURE NO.</b>	<b>TITLE</b>	<b>PAGE</b>
<b>Figure 1.1</b>	Smart farming architectures (Quy et al., 2022).	<b>6</b>
<b>Figure 2.1</b>	The structure of IoT in smart farming (Rettore et al., 2020)	<b>21</b>
<b>Figure 2.2</b>	The different layers of IoT architectures.	<b>24</b>
<b>Figure 2.3</b>	An overview of access control flows (Bertin et al., 2018)	<b>46</b>
<b>Figure 2.4</b>	The basic concept of RBAC model (Malik et al., 2020)	<b>52</b>
<b>Figure 2.5</b>	The basis of ABAC model (Aghili et al., 2022)	<b>55</b>
<b>Figure 2.6</b>	FRABAC model (Attia et al., 2018)	<b>60</b>
<b>Figure 2.7</b>	Process of blockchain technology to complete a transaction.	<b>72</b>
<b>Figure 2.8</b>	Formation of blocks in a blockchain	<b>74</b>
<b>Figure 2.9</b>	Smart Contract Process	<b>78</b>
<b>Figure 2.10</b>	Mechanism of Gas in Ethereum Network (Ma et al., 2019)	<b>88</b>
<b>Figure 3.1</b>	Decentralised access control framework for IoT security by leveraging blockchain technology	<b>122</b>
<b>Figure 3.2</b>	Smart contract-based access control model.	<b>131</b>
<b>Figure 3.3</b>	Step-by-step for formatting access policy	<b>136</b>
<b>Figure 3.4</b>	The components for developing access policies for IoT devices in smart farming.	<b>137</b>
<b>Figure 3.5</b>	Hierarchical role in smart farming	<b>138</b>
<b>Figure 3.6</b>	Sample policy 1.	<b>139</b>

<b>Figure 3.7</b>	Example scenario of sample policy 2	<b>140</b>
<b>Figure 3.8</b>	Sample policy 2.	<b>141</b>
<b>Figure 3.9</b>	Sample policy 3.	<b>143</b>
<b>Figure 3.10</b>	Sample policy 4.	<b>144</b>
<b>Figure 3.11</b>	Research Methodology.	<b>145</b>
<b>Figure 3.12</b>	Research Design of this Study.	<b>149</b>
<b>Figure 3.13</b>	Experimental Design.	<b>154</b>
<b>Figure 3.14</b>	The Hardware and Software in the Case Study. there are three laptops, two acting as a light node of subject and object, and a miner node acting as a gateway proxy node.	<b>156</b>
<b>Figure 3.15</b>	The interaction between the contract owner and IoT requestor node with smart contracts to access a resource.	<b>159</b>
<b>Figure 3.16</b>	The algorithm for IoT_ORMC.	<b>161</b>
<b>Figure 3.17</b>	The algorithm for IoT_SRMC.	<b>164</b>
<b>Figure 3.18</b>	The algorithm for IoT_ACC.	<b>168</b>
<b>Figure 3.19</b>	Execution process for the implemented case study.	<b>169</b>
<b>Figure 3.20</b>	Snapshot of the interface for registering a new device with id and other attributes.	<b>170</b>
<b>Figure 3.21</b>	Snapshot of the interface for adding resources to the blockchain network.	<b>171</b>
<b>Figure 3.22</b>	Snapshot of the interface for access request form.	<b>172</b>
<b>Figure 3.23</b>	Snapshot of Ganache accounts.	<b>172</b>
<b>Figure 4.1</b>	The response of Remix IDE after a transaction completion.	<b>182</b>

<b>Figure 4.2</b>	The result of the access permission request denied in Remix IDE.	<b>182</b>
<b>Figure 4.3</b>	Snapshot of error access denied in unmatching attributes devices.	<b>183</b>
<b>Figure 4.4</b>	Calculation for the cost consumption.	<b>185</b>
<b>Figure 4.5</b>	Calculation for conversion factor from wei to ETH.	<b>185</b>
<b>Figure 4.6</b>	The deployment cost consumption.	<b>186</b>
<b>Figure 4.7</b>	Gas used and type of function in managing attributes and role of the subject in each function within proposed schemes.	<b>190</b>
<b>Figure 4.8</b>	Gas used and type of function in managing attributes and role of object in each function within existing proposed schemes.	<b>193</b>
<b>Figure 4.9</b>	Gas used in managing access policy in each function within proposed schemes.	<b>195</b>
<b>Figure 4.10</b>	The number of transaction requests over time (ms) with different functions of contracts.	<b>199</b>
<b>Figure 4.11</b>	Average throughput with varying number of transactions request in the different function of contracts.	<b>202</b>
<b>Figure 4.12</b>	Average latency with varying number of transactions (10,100,150) of different function.	<b>203</b>
<b>Figure 4.13</b>	An error during request transaction in the Sepolia network.	<b>208</b>

## 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