UNIVERSITI PUTRA MALAYSIA

SECURE MULTI-AUTHORITY ATTRIBUTE-BASED ENCRYPTION ACCESS CONTROL WITH CACHE-AWARE SCHEDULING IN MOBILE CLOUD COMPUTING

FARA BINTI JAMAL

FSKTM 2021 2

SECURE MULTI-AUTHORITY ATTRIBUTE-BASED ENCRYPTION ACCESS CONTROL WITH CACHE-AWARE SCHEDULING IN MOBILE CLOUD COMPUTING

By

FARA BINTI JAMAL

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfilment of the Requirements for the Degree of Doctor of Philosophy

March 2021

DEDICATION

This thesis is dedicated to my beloved father, mother, husband, daughters and son.
Thank you for all the prayers.

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Doctor of Philosophy

SECURE MULTI-AUTHORITY ATTRIBUTE-BASED ENCRYPTION ACCESS CONTROL WITH CACHE-AWARE SCHEDULING IN MOBILE CLOUD COMPUTING

By

FARA BINTI JAMAL

March 2021

Chairman : Associate Professor Mohd Taufik Abdullah, PhD
Faculty : Computer Science and Information Technology

Mobile Cloud Computing (MCC) is the combination of cloud computing, mobile computing, and wireless network to bring rich computational resources to mobile users, network operators, as well as cloud computing providers. MCC has raised various security concerns and delayed access due to hosting sensitive data on an untrusted cloud environment, and the control over such data by their owners is lost after uploading to the cloud. Fine-grained access control using Attribute-Based Encryption (ABE) mechanisms can be enforced as the first line of defense on the untrusted cloud to forbid unauthorized access to the stored data.

Some schemes have been proposed to deliver such access control using Ciphertext-policy attribute-based encryption (CP-ABE) that can enforce data owners' access policies to achieve such cryptographic access control and tackle the majority of those concerns. However, some challenges are still outstanding due to the complexity of frequently changing the cryptographic enforcements of the owners' access policies in the hosted cloud data files, and the key issuing process which poses computational and communicational overheads to data owners. These challenges are: 1) single point failure in the cryptography scheme, 2) key abuse problem in the key generating process, and 3) delayed access to the data in the cloud for the user.

This thesis analyzed some of the existing, related issues and proposed a scheme that extends the relevant existing techniques to resolve the inherent problems in CP-ABE without incurring heavy computation overhead. In particular, the Certificate Authority is a single entity that leads to a single point of failure, while the Attribute Authority works independently. A user's secret key to acquire data from the cloud will not be generated if there is a failure in one of the Attribute Authority's nodes. The proposed scheme offers a solution to perform a novel technique using a neighbor node backup

concept that will minimize the mean downtime and increase the availability of the scheme during the failure of one or more authority nodes. Each authority node will have a failover node that will take over the failed node function to maintain the scheme operation.

Furthermore, in all ABE schemes, a single point of failure runs in a centralized storage manner, which in return may collapse the system. Although the key generator is distributed among the authority nodes, the decision to generate user credential is based on a single decision. An adversary can force the authority to produce false private keys that can tarnish the integrity of the ABE system. To achieve the integrity of the scheme, this research proposed a decentralized attribute storage and authority consensus by lowering the Mean Time To Detect (MTTD) and maintaining the new storage count during a security attack. Also, user attributes are stored in the block storage using an InterPlanetary File System (IPFS) protocol to eliminate the concept of centralizing storage.

In addition, during peak hours, increasing requests from mobile devices to the cloud storage will result in network congestion and significant delays for the cloud to entertain user requests which can cause the required data to become unavailable. By leveraging the existing work, a cache-aware scheduling technique was developed to minimize communication and read time between cloud storage and the mobile device to reduce the unavailability of required data.

The proposed scheme experiment showed that the scheme managed to overcome the limitations on the existing solution. The result indicated that the Mean Downtime Time for the proposed solution was only 3.88 minutes compared to the existing solution, which was 38.56 minutes. During a security attack, the MTTD for the existing solution was very high because the existing scheme could not detect the attack. For the proposed scheme, the MTTD was very low which is 4.89 minutes, because of the consensus algorithm. Furthermore, by using the cache-aware scheduling, the proposed scheme managed to save 2.18% reads more than those of the existing work solution; this could reduce the time taken to access required data. The proposed Multi-Authority Attribute-Based Encryption with Cache-Aware Scheduling for Mobile Cloud Access Control in Mobile Cloud Computing environment analysis of the theoretical and implemented results demonstrated that the scheme performed better compared to the previous work solution in terms of availability and integrity. The proposed schemes were carefully designed to minimize computation and communication overhead to suit the device's resource constraint in MCC.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Doktor Falsafah

KAWALAN CAPAIAN PENYULITAN SELAMAT BERASASKAN ATRIBUT PELBAGAI AUTORITI DENGAN PENJADUALAN SEDAR-CACHE DALAM KOMPUTERAN AWAN BERGERAK

Oleh

FARA BINTI JAMAL

Mac 2021

Pengerusi : Profesor Madya Mohd Taufik Abdullah, PhD
Fakulti : Sains Komputer dan Teknolologi Maklumat

Pengkomputeran awan bergerak (MCC) adalah istilah yang digunakan untuk khidmat luaran data sensitif kepada persekitaran awan yang kurang dipercayai dan membolehkan capaian daripada peranti mudah alih. MCC telah membangkitkan pelbagai masalah keselamatan dan kelewatan capaian disebabkan oleh pengehosan data sensitif pada persekitaran awan yang tidak dipercayai, dan kawalan ke atas data tersebut oleh pemiliknya hilang setelah memuat naik ke awan. Kawalan capaian yang terperinci yang menggunakan mekanisme Penyulitan Berasaskan Atribut (ABE) dapat dikuatkuasa sebagai barisan pertahanan pertama pada awan untuk melarang capaian tanpa izin ke data yang disimpan.

Beberapa teknik telah diusulkan untuk melaksanakan kawalan akses dengan menggunakan penyulitan berdasarkan atribut teks sifer (CP-ABE) yang dapat menguatkuasa polisi capaian pemilik data untuk mencapai kawalan capaian kriptografi tersebut dan mengatasi sebahagian besar masalah yang dihadapi. Walaubagaimanapun, beberapa cabaran masih belum selesai disebabkan oleh kompleksiti kerana kerap menukar penguatkuasaan kriptografi polisi capaian pemilik dalam fail data awan yang dihoskan, dan proses terbitan kunci yang mempunyai overhed pengkomputeran dan komunikasi kepada pemilik data. Cabaran ini adalah: 1) kegagalan satu titik dalam teknik penyulitan, 2) masalah penyalahgunaan kunci dalam proses penjanaan kunci, dan 3) melambatkan akses ke data di awan dari pengguna.

Tesis ini menganalisa beberapa masalah yang berkaitan dan sedia ada, dan mencadangkan skema yang memperluaskan teknik-teknik sedia ada untuk menyelesaikan masalah yang wujud dalam CP-ABE tanpa menanggung overhed pengkomputeran yang tinggi. Khususnya, Autoriti Perakuan (*Certificate Authority*) adalah satu entiti yang merujuk kepada titik kegagalan tunggal, sementara Autoriti

Atribut (*Attribute Authority*) berfungsi secara bebas. Kunci rahsia pengguna untuk memperoleh data daripada awan tidak akan dihasilkan sekiranya terdapat kegagalan di salah satu nod Autoriti Atribut. Skema yang dicadangkan mengemukakan penyelesaian untuk menjalankan teknik baharu menggunakan konsep sandaran nod tetangga (*failover node)* . Setiap nod autoriti mempunyai nod sandaran yang akan mengambil alih fungsi nod yang gagal untuk mengekalkan operasi skema.

Tambahan lagi, dalam kesemua skema ABE, titik kegagalan tunggal bergerak dengan cara penyimpanan berpusat, yang sebaliknya boleh meruntuhkan sistem tersebut. Walaupun penjana kunci diedarkan di antara nod autoriti, keputusan untuk menghasilkan akuan pengguna adalah berdasarkan keputusan tunggal. Penggodam boleh memaksa autoriti tersebut untuk menghasilkan kunci peribadi palsu yang boleh mencemarkan integriti sistem ABE. Bagi meningkatkan integriti sistem, kajian ini mencadangkan pelaksanaan storan atribut secara tidak berpusat dan autoriti konsensus supaya dapat mengurangkan purata masa pengesanan serangan dan mengekalkan pertambahan storan baru sekiranya berlaku serangan keselamatan. Atribut pengguna pula di simpan dalam storan blok menggunakan protokol *InterPlanetary File System* (IPFS) untuk menghapuskan konsep storan berpusat.

Di samping itu, pada waktu puncak, permintaan yang meningkat dari peranti mudah alih ke storan awan akan menyebabkan kesesakan rangkaian dan kelewatan capaian yang signifikan bagi awan untuk melayan permintaan pengguna yang boleh menyebabkan data yang diperlukan menjadi tidak tersedia. Dengan menambahbaik kajian yang ada, teknik Penjadualan Sedar-Cache dibangunkan untuk meminimumkan komunikasi dan masa capaian antara storan awan dan peranti mudah alih untuk mengurangkan kadar ketidaksediaan data yang diperlukan.

Eksperimen yang telah dilaksanakan membuktikan sistem yang dibangunkan dapat mengurangkan kekangan yang terdapat pada teknik sedia ada. Keputusan pengujian menunjukkan purata masa tergendala bagi sistem cadangan hanyalah 3.88 minit berbanding 38.56 minit bagi sistem sedia ada. Semasa berlaku serangan keselamatan, purata masa pengesanan serangan bagi teknik sedia ada adalah sangat tinggi kerana tidak dapat mengenal pasti serangan berbanding teknik yang dicadangkan yang hanya mengambil masa 4.89 minit untuk mengenal pasti serangan kerana adanya algoritma konsensus. Selain itu, teknik yang dicadangkan dapat mengurangkan sebanyak 2.18% capaian ke storan awan berbanding teknik sedia ada yang seterusnya dapat mengurangkan masa capaian data yang diperlukan oleh pengguna. Analisis dan pelaksanaan mekanisme Kawalan Capaian Penyulitan Selamat Berasaskan Atribut Pelbagai Autoriti Dengan Penjadualan Sedar-Cache Dalam Komputeran Awan Bergerak membuktikan teknik ini menunjukkan prestasi yang lebih baik berbanding teknik sedia ada dari segi ketersediaan dan integriti. Skema yang dicadangkan direka bentuk dengan teliti untuk meminimumkan overhed pengkomputeran dan komunikasi supaya sesuai dengan kekangan sumber peranti di MCC.

ACKNOWLEDGEMENTS

First and foremost, I wish to express my profound gratitude to Almighty Allah SubhanahuWa Taala for the courage, strength, guidance, patience, and making it possible for me to finish this research. I thank Allah for His immense grace and blessing for every stage of my entire life. May blessings and peace be upon Prophet Muhammad Sallalahu AlaihiWasallam, who was sent for mercy to the entire world.

I am indebted to my supervisor, Assoc.Prof. Dr. Mohd Taufik Abdullah who stood firm to encourage and guide me throughout this research journey. Thanks to my dedicated committee members (Assoc. Prof. Dr. Zurina Mohd Hanapi and Assoc. Prof. Dr. Azizol Abdullah), who were ever ready to put forward useful advices to ensure the progress of this research.

I would like to express my appreciation to my loving husband, Faizal, my kids, Fiesya Irdina, Fahri Irsyad and Finna Irisya. It would have been impossible for me to finish this study without their understanding and support. Honour goes to my parents Jamal and Che Sham, without whose undying encouragements and belief in me, I would have never dreamt of such an achievement in life. Special thanks go to my colleagues and friends for the support and prayers throughout these years. Finally, I would like to acknowledge every individual for his or her invaluable help, and cooperation throughout my research.

I thank Allah truly for these blessings.

"Keep Your Eyes On The Stars, But Your Feet On The Ground"- Theodore Roosevelt

This thesis was submitted to the Senate of the Universiti Putra Malaysia and has been accepted as fulfilment of the requirement for the degree of Doctor of Philosophy. The members of the Supervisory Committee were as follows:

Mohd Taufik bin Abdullah, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

Azizol bin Abdullah, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

Zurina binti Mohd Hanapi, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

ZALILAH MOHD SHARIFF, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 9 September 2021

Declaration by graduate student

I hereby confirm that:

- this thesis is my original work;
- quotations, illustrations and citations have been duly referenced;
- this thesis has not been submitted previously or concurrently for any other degree at any institutions;
- intellectual property from the thesis and copyright of thesis are fully-owned by Universiti Putra Malaysia, as according to the Universiti Putra Malaysia (Research) Rules 2012;
- written permission must be obtained from supervisor and the office of Deputy Vice-Chancellor (Research and innovation) before thesis is published (in the form of written, printed or in electronic form) including books, journals, modules, proceedings, popular writings, seminar papers, manuscripts, posters, reports, lecture notes, learning modules or any other materials as stated in the Universiti Putra Malaysia (Research) Rules 2012;
- there is no plagiarism or data falsification/fabrication in the thesis, and scholarly integrity is upheld as according to the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) and the Universiti Putra Malaysia (Research) Rules 2012. The thesis has undergone plagiarism detection software

Signature: _____ Date: _____

Name and Matric No: Fara binti Jamal, GS48380

Declaration by Members of Supervisory Committee

This is to confirm that:

- the research conducted and the writing of this thesis was under our supervision;
- supervision responsibilities as stated in the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) were adhered to.

Signature:	_____
Name of Chairman of Supervisory Committee:	Associate Professor Dr. Mohd Taufik Abdullah
Signature:	_____
Name of Member of Supervisory Committee:	Associate Professor Dr. Azizol Abdullah
Signature:	_____
Name of Member of Supervisory Committee:	Associate Professor Dr. Zurina Mohd Hanapi

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF NOTATIONS

i	AA Secret Key
$\mathbb{T}$	Access Structure
$\mathbb{S}$	Attributes
A_I	Authority Agent
Y	Authority Public Key
e	Bilinear Map
z	Child Nodes
$\mathbb{CT}$	Ciphertext
$\mathbb{G}_1$	Cyclic Group
B	Data Owner
ε	Elliptic Curve
$\perp$	Error
FN_i	Failover Node
$\mathbb{F}_p$	Finite Field
g	Generator
$\mathbb{GP}$	Global Parameter
$\mathbb{Y}$	Group of Leaf Nodes
$\mathbb{H}(j)$	Hash Function
x	Leaf Node
$\mathbb{MK}$	Master Key
$\mathbb{M}$	Message
$\boldsymbol{v}$	Number Of Authority

N_I	Primary Node
p	Prime Order
$\mathbb{SK}$	Secret Key
$\mathbb{PK}$	Public Key
$\mathbb{R}$	Root Node
α, β	Security Parameter
k_x	Threshold Value
$\mathbb{N}$	Total Number of Attribute
F	Total Number of Data Owner
N	Total Number of User
C	User
WA	Weight

LIST OF ABBREVIATIONS

AA	Attribute Authority
ABAC	Attribute-Based Access Control
ABE	Attribute-Based Encryption
AP	Access Point
ARBAC	Attribute And Role-Based Access Control
BD	Block Data
CA	Certification Authority
CCP-CABE	Comparative CP-ABE
CP-ABE	Ciphertext-Policy Attribute-Based Encryption
CS	Cloud Server
CSA	Client Site Agent
CSP	Cloud Service Providers
CSS	Client Storage Server
DAC	Discretionary Access Control
DAG	Directed Acyclic Graph
DoS	Denial of Services
DHT	Distributed Hash Tables
DO	Data Owner
DU	Data User
EACDAC	Effective Attribute-Based Comparable Data Access Control
ECC	Elliptic Curve Cryptography
ECDDH	Elliptic Curve Decisional Diffie-Hellman
ESACSM	Efficient And Secure Access Control System

FGAC	Fine-Grained Access Control
FN	Failover Node
HABAC	Hierarchical Attribute-Based Access Control
HABE	Hierarchical Attribute-Based Encryption
IBE	Identity-Based Encryption
IoT	Internet Of Things
IPFS	Interplanetary File System
KP-ABE	Key Policy Attribute-Based Encryption
LSSS	Linear Secret Sharing Scheme
MA	Multiple Authority
MAC	Mandatory Access Control
MCC	Mobile Cloud Computing
MD	Mobile Devices
MDT	Mean Downtime
MK	Master Key
MTTD	Mean Time To Detect
NSC	New Storage Count
P2p	Peer-To-Peer
PADMC	Privacy-Aware Authentication Scheme For Distributed Mobile Cloud Computing
PBC	Pairing-Based Cryptography
PK	Public Key
PKC	Public-Key Cryptography
PN	Prime Node
QoS	Quality Of Service

RBAC	Role-Based Access Control
RBE	Role-Based Encryption Access Control Model
RDC	Remote Data Center
RMTAC	Reputation-Based MCC Storage And System Architecture
SCG	Smart Card Generator
SSA	Server Site Agent
UPP	User Preference Profile

CHAPTER 1

INTRODUCTION

Organizations have traditionally used local servers to store data, while company employees would use organization devices with enabled apps to access data. For protection, control has been established by organizations to control the data access. The practice has now shifted, as users may access corporate data from anywhere and at any time via mobile devices like smartphones, personal computers, and tablets. On the other side, through technological advances, the way of storing, exchanging, accessing, and manipulating data has improved. Organizations and individuals are continually motivated to use technologies that enable data exchange, openness, and availability from all areas of the world. The cloud is a proven technology that provides this form of service. The combination of cloud storage with the use of mobile device derives the term Mobile Cloud Computing. Mobile Cloud Computing (MCC) has now been widely implemented, enabling mobile devices to access data processed in the cloud (A.Elgendy, Zhang, Liu, & Hsu, 2021; Aliyu et al., 2020).

Through MCC, data is stored and analysed in the cloud to increase the ability of mobile devices. As it requires a third-party system (cloud service provider) that does not guarantee data confidentiality, the concern regarding MCC is mainly on security and privacy (R. Kumar, 2020). In fact, if data stored on the public cloud is not encrypted, it can be exposed (Merdassi, Ghazel, & Saidane, 2020; Sun, 2019). The first line of protection that will block unauthorized data access in an untrusted environment can be implemented by utilizing the Attribute-Based Encryption (ABE) access control technique.

ABE is a robust encryption approach that maintains the security of information and access control that are suitable for Mobile Cloud Computing (Sun, 2020; S. Xu, Yang, Mu, & Deng, 2018). The ABE schemes implemented by (Hu, Kuhn, & Ferraiolo, 2015), and (Zhibin Zhou, Huang, & Wang, 2013) are the strongest encryption mechanisms, where authentication is based on the ciphertext, whereas the user's secret keys are connected to attribute sets. A user has to be verified by multiple authorities in order to perform encryption and decryption. The authorities are the Certification Authority (CA) and Attribute Authority (AA). CA reviews and certifies the user, while AA looks for the authenticity of the user's attributes, and depending on the credentials from CA, AA will issue the secret keys for user to encrypt and decrypt data in the cloud.

The current ABE technique that has been used in an MCC environment has issues in terms of availability and integrity (Salman, Zolanvari, Erbad, Jain, & Samaka, 2019). The technique is prone to attack and can cause a single point failure. In such circumstances, building security mechanisms using ABE to ensure continuality and reliable access control is mandatory since the confidentiality of data in the cloud relies on it. Unfortunately, mobile resource constraints is a major obstacle towards the

implementation of secure access control techniques, thus making defense a more challenging aspect of the MCC environment (Albulayhi, Abuhussein, Alsubaei, & Sheldon, 2020; Y. Zhang et al., 2020). Researchers now focus on addressing this issue by building models that would perform a similar task to traditional access control but less demanding on the constrained resources.

This research used a technique by (N. Agrawal & Tapaswi, 2019) as a benchmark. The proposed technique will fill in the gap of the technique by (N. Agrawal & Tapaswi, 2019) that had issues in terms of availability and integrity of the ABE scheme. Therefore, this research concentrated on the security of access control technique using encryption technology and the accessibility between mobile devices and the cloud to leverage the benefits of the technologies mentioned above while minimizing the resource constraint. In this chapter, the research problem is presented in Section 1.1, while Sections 1.2, 1.3, and 1.4 explain the motivation, objectives, and scope. Finally, Section 1.5 shows the outline of the thesis.

1.1 Research Problem

Crucial, vast, and scalable data that are stored in a cloud environment require a safe means to defend and maintain its uprightness and privacy without impacting the accessibility and availability of the system. One of the essential data protection security systems are the attribute-based encryption (ABE) access control system, which enables, limits, or prevents approach to user data by making certain requirements and policy that are joined to form and implement controlling decisions (Fugkeaw, 2021).

Although many works have been carried out using the ABE access control in MCC environment, such studies have numerous unresolved challenges. For example, some researchers proposed a scheme with a low computation overhead that is suitable for mobile constraints, but the study identified some security issues (Arthur Sandor, Lin, Li, Lin, & Zhang, 2019; Y. Liu, Zhang, Ling, & Liu, 2018). On the other hand, in exchange for improved security protection, certain schemes required intensive computation, which would not be ideal for devices with a limited processing capacity (Z. Wu, Zhang, & Xu, 2020; X. Zhang, Wu, Yao, Wang, & Wang, 2019).

Much of the ABE works such as a work from (N. Agrawal & Tapaswi, 2019; Al-dahhan, Shi, Lee, & Kifayat, 2018; Z. Wu et al., 2020; M. Xie, Ruan, Hong, & Shao, 2021; Y. Xie, Wen, Wu, Jiang, & Meng, 2019) focused on data confidentiality in the untrusted cloud rather than the integrity and availability of the ABE scheme. While encrypted data is confidential and can only be accessed by an authorized user, if the ABE access control mechanism is not available, the user is still unable to access data in the cloud. There is also a lack of research on the integrity of the ABE access control mechanism to encrypt and decrypt data in the cloud (R. Kumar, 2020; Merdassi et al., 2020). Most researchers presumed the integrity of the scheme in the security assumption without implementing tests and validations. There are three unsolved challenges related to the availability and integrity of data in the MCC environment with ABE access control, which include:

- The first challenge is related to the ABE authorities, namely the Certification Authority (CA) and Attribute Authority (AA). On cloud storage, encrypted data can be stored using an ABE scheme, and it can be done based on the decision by CA and AA whether to grant access to the user. The CA verifies user identity and generates the credentials. The credentials are passed to AA to generate a secret key. CA is a single entity that can lead to a single point of failure. If CA fails to generate the credentials, AA cannot generate a secret key. On the other hand, although there are multiple AAs in the scheme, each AA works independently. Each AA is responsible in verifying their respective attributes then generate a partial key (N. Agrawal & Tapaswi, 2018). If one or more AA fails, the partial key would not be completed thus, a secret key cannot be generated. As a result, the ABE scheme will be unavailable, and the user fails to access their required data in the cloud (Al-dahhan, Shi, Lee, & Kifayat, 2018; Al-Dahhan, Shi, Lee, & Kifayat, 2019; F. Li, Rahulamathavan, Conti, & Rajarajan, 2015; Salman et al., 2019).

- Moreover, in an ABE scheme, such as in (N. Agrawal & Tapaswi, 2018) technique, the user's static and dynamic attributes are stored on the local centralized server or centralised storage in the cloud. A single point of failure runs in a centralized storage manner, which in return, may collapse the system (Sukhodolskiy & Zapechnikov, 2018; Shangping Wang, Zhang, & Zhang, 2018). Furthermore, all data stored in the cloud server can be decrypted by the key generator for the ABE scheme, which is the certification authority and attributes authority. Some of the major problems, such as key abuse and data privacy leakage, could be caused by this (R. Kumar, 2020). Although the key generator is distributed among the authority's nodes, the decision to generate user credential is based on one central entity, and each attribute authority has the full decision to generate a partial key. If an adversary takes over one of the authority nodes, they can be forced to generate a partial key and produce false secret keys that can tarnish the integrity of the ABE system (A. Wu et al., 2019).

- In an MCC environment, user can access data in the cloud using their mobile device. It provides safe and quick access to the data. However, during peak hours, increasing requests from mobile devices to the cloud storage will result in network congestion and a remarkable delay for the cloud to entertain user requests. Peak-time traffic increased by approximately 50 percent and will keep growing at high speed (Cisco, 2019; Zhenyu Zhou et al., 2020). A large number of users using their mobile device who repeatedly request a particular content in a short period of time will put high pressure on the cloud and the network (Bakiras, Troja, & Xu, 2020). This can cause the required data to become unavailable.

From the aforementioned problems, it is clear that there is a limitation in the existing ABE access control scheme in terms of scheme availability and integrity for storing and accessing data in the untrusted cloud. The same issues are the gap of the benchmark (N. Agrawal & Tapaswi, 2019) solution. The issues are related to authority node, attribute storage, key issuing mechanism and data access from mobile to the cloud. This research aims to improve the ABE access control scheme by eliminating the mentioned problem,

hence improve the availability and integrity of the scheme while minimizing the computation overhead to suit the MCC environment.

1.2 Motivation

Based on the problems described above, the motivation of this research is to create a scheme that has a minimum downtime which ensures reliable storage and sharing of empathetic data in the cloud in a particular way that enhances the decision-making stage for accessing its assets. The goal would be helpful for certain mobile cloud platforms with digital content, e.g., videos, government documents, etc. Such applications are becoming regular in the cloud era, and a technique is needed to keep data from being accessed by unauthorized users.

Due to changes in the access policy, providing a new scheme for customizable access to cloud resources would provide data owners with better flexibility and protection; allowing them to share resources with others for simpler access. The purpose of this research is to consider current research in mobile cloud access control methodologies, and subsequently, to construct a new, scalable, secure access control model. Although several studies have been carried out in this area, little research has gone through all of the issues listed above in improving the decision-making method for controlling accessibility to cloud environments while maintaining the availability and integrity of the needed information.

1.3 Research Objectives

The main objective of this research is to propose a secure Access Control Scheme using Multi-authority Attribute-Based Encryption approaches that are aimed to ensure the availability and integrity while minimizing computational overhead that is suitable for Mobile Cloud Computing. To achieve this, the following objectives are considered:

1. To propose a reliable authority agent using the failover node concept that will minimize the mean downtime and increase the availability of the scheme during failure of one or more authority nodes. The scheme is expected to continue providing access control mechanism for a user to access data in the cloud even during a security attack. The proposed scheme will solve the first problem described in Section 1.1 which is a single point failure in the authority.

2. To propose a distributed attribute storage and authority consensus to increase the integrity of the scheme by lowering the Mean Time To Detect (MTTD) and maintain the new storage count during a security attack. The scheme is expected to detect an attack and prevent it from tempering with the key issuing process. The proposed scheme will solve the second problem described in Section 1.1 which is a single point failure in the centralized server and key abuse among authority.

3. To propose a cache-aware scheduling technique by improving the existing cache-based process to minimize communication time and read between cloud storage and the mobile device; hence, reducing the unavailability of the required data. The proposed scheme will solve the third problem described in Section 1.1 which is data unavailability during peak hours.

1.4 Research Scope

Numerous researchers have proposed various ABE methods, such as Fuzzy Identity-based, symmetric encryption algorithm, and attribute-based. This research proposed an ABE technique focusing on using an attribute-based method that only relates to authorities' nodes, issuing key and accessing the cloud. Although there are issues in the revocation process, this thesis does not focus on that area. Some researchers have used advanced methods, such as blockchain, to secure the ABE scheme, but this research focused on using the present environment that does not require high computing resources suitable for mobile cloud computing.

This research focused on ABE access control in Mobile Cloud Computing. There are ABE access control mechanisms proposed by previous researchers (Di, Maesa, Mori, Ricci, & Nazionale, 2019; Dias, Sereno Ferreira, & Martins, 2020; Ding, Cao, Li, Fan, & Li, 2019; Madine et al., 2020; Omar et al., 2020; Tanwar, Parekh, & Evans, 2020; J. Xu et al., 2019) to access data in the cloud, but these imposed a high computation overhead that may be suitable for other environments. For MCC, the device resource is the limitation that needs to be looked into in designing an access control mechanism. This research developed a mechanism that increases security but with minimal use on the mobile device resourced.

The proposed approaches were tested using a simulation tool, extensively under various threats (in the case of security attacks). The schemes were enhanced and further provided a better trade-off for both computation overhead and security performance.

1.5 Thesis Organization

The subsequent thesis chapters are structured as follows:

Chapter 2 presents the related definitions, basics, and principles of the ABE scheme. Besides that, several issues and restrictions are identified in the related work.

Chapter 3 briefly presents the methodology, some mathematical backgrounds, relevant principles, and fundamental ideas of advanced cryptographic techniques, as well as a simulation of the base work scheme.

Chapter 4 proposes a new High-availability Multi-authority Attribute-Based Encryption scheme with a failover node that eliminates a single point of failure in authority. The theoretical model is subsequently presented. Towards the end of this chapter, based on the scheme evaluation and experimental results, the scheme was analysed in terms of security and performance to show that the proposed scheme is secure against attacks.

Chapter 5 proposes a new Decentralized Attribute Storage with Authority Consensus scheme that eliminates the point of attack on the storage and centralized decision on the authority. Besides that, this chapter presents the scheme implementation and discusses the test results. Also, a correlation between the proposed scheme and the base work was done to check the effectiveness of the proposed scheme.

Chapter 6 broadens the work from previous works by proposing a cache-aware scheduling scheme that enhances the current cache technique. The implementation, testing, and evaluation are discussed in this chapter to show that the proposed solution is better in maintaining data availability and speeding up the access process between the mobile device and the cloud.

Chapter 7 summarizes all the chapters and concludes the thesis. Also, it points out several directions for potential future research, following the results extracted from this work.

REFERENCES

A.Elgendy, I., Zhang, W.-Z., Liu, C.-Y., & Hsu, C.-H. (2021). An efficient and secured framework for mobile cloud computing. *IEEE Transactions on Cloud Computing*, *9*(1). https://doi.org/10.35940/ijitee.I7562.0981119

Abbasi, M., Yaghoobikia, M., Rafiee, M., Jolfaei, A., & Khosravi, M. R. (2020). Energy-efficient workload allocation in fog-cloud based services of intelligent transportation systems using a learning classifier system. *IET Intelligent Transport Systems*, *14*(11), 1484–1490. https://doi.org/10.1049/iet-its.2019.0783

Abdel-Basset, M., Mohamed, R., Elhoseny, M., Bashir, A. K., Jolfaei, A., & Kumar, N. (2021). Energy-Aware Marine Predators Algorithm for Task Scheduling in IoT-Based Fog Computing Applications. *IEEE Transactions on Industrial Informatics*, *17*(7), 5068–5076. https://doi.org/10.1109/TII.2020.3001067

Aftab, M. U., Qin, Z., Zakria, Ali, S., Pirah, P., & Khan, J. (2019). The Evaluation and Comparative Analysis of Role Based Access Control and Attribute Based Access Control Model. *2018 15th International Computer Conference on Wavelet Active Media Technology and Information Processing, ICCWAMTIP 2018*, 35–39. https://doi.org/10.1109/ICCWAMTIP.2018.8632578

Agrawal, N., & Tapaswi, S. (2018). Access Control Framework Using Dynamic Attributes Encryption for Mobile Cloud Environment. In *Advances in Intelligent Systems and Computing* (pp. 611–621). Springer Nature Singapore Pte Ltd.

Agrawal, N., & Tapaswi, S. (2019). A trustworthy agent-based encrypted access control method for mobile cloud computing environment. *Pervasive and Mobile Computing*, *52*, 13–28. https://doi.org/10.1016/j.pmcj.2018.11.003

Agrawal, S., & Chase, M. (2017). FAME : Fast Attribute-based Message Encryption. In *SIGSAC Conference on Computer and Communications Security* (pp. 665–682). ACM.

Ahlehagh, H., & Dey, S. (2017). Video-Aware Scheduling and Caching in the Radio Access Network. *IEEE Transactions on Networking*, *22*(5), 1444–1462.

Ahmad, A. A. S., Brereton, P., & Andras, P. (2017). A Systematic Mapping Study of Empirical Studies on Software Cloud Testing Methods. *Proceedings - 2017 IEEE International Conference on Software Quality, Reliability and Security Companion, QRS-C 2017*, 555–562. https://doi.org/10.1109/QRS-C.2017.94

Al-Ahmad, A. S., Kahtan, H., Hujainah, F., & Jalab, H. A. (2019). Systematic Literature Review on Penetration Testing for Mobile Cloud Computing Applications. *IEEE Access*, *7*, 173524–173540. https://doi.org/10.1109/ACCESS.2019.2956770

Al-dahhan, R. R., Shi, Q., Lee, G. M., & Kifayat, K. (2018). Revocable , Decentralized Multi-authority Access Control System. In *2018 IEEE/ACM International Conference on Utility and Cloud Computing Companion (UCC Companion)* (pp. 220–225). IEEE. https://doi.org/10.1109/UCC-Companion.2018.00088

Al-Dahhan, R. R., Shi, Q., Lee, G. M., & Kifayat, K. (2019). Survey on Revocation in Ciphertext-Policy Attribute-Based Encryption. *Sensors*, 1–22.

Al-Janabi, S., Al-Shourbaji, I., Shojafar, M., & Abdelhag, M. (2018). Mobile Cloud Computing: Challenges and Future Research Directions. *Proceedings - International Conference on Developments in ESystems Engineering, DeSE*, (June), 62–67. https://doi.org/10.1109/DeSE.2017.21

Albulayhi, K., Abuhussein, A., Alsubaei, F., & Sheldon, F. T. (2020). Fine-Grained Access Control in the Era of Cloud Computing: An Analytical Review. *2020 10th Annual Computing and Communication Workshop and Conference, CCWC 2020*, 748–755. https://doi.org/10.1109/CCWC47524.2020.9031179

Aldmour, R., Yousef, S., Baker, T., & Benkhelifa, E. (2021). An Approach for Offloading in Mobile Cloud Computing to Optimize Power Consumption and Processing Time. *Sustainable Computing: Informatics and Systems*, *31*(May), 100562. https://doi.org/10.1016/j.suscom.2021.100562

Ali, W., Shamsuddin, S. M., & Ismail, A. S. (2011). A Survey of Web Caching and Prefetching. *Int. J. Advance. Soft Comput. Appl.*, *3*(1), 1–27.

Aliyu, A., Abdullah, A. H., Kaiwartya, O., Hamid, S., Madni, H., Joda, U. M., … Tayyab, M. (2020). Mobile Cloud Computing : Taxonomy and Challenges. *Journal of Computer Networks and Communication*, *2020*.

Alizadeh, M., & Hassan, W. H. (2020). Challenges and opportunities of mobile cloud computing. *9th International Wireless Communications and Mobile Computing Conference, IWCMC*, (May), 660–666. https://doi.org/10.1109/IWCMC.2013.6583636

Almarhabi, K., Jambi, K., Eassa, F., & Batarfi, O. (2018). A Proposed Framework for Access Control in the Cloud and BYOD Environment. *IJCSNS International Journal of Computer Science and Network Security*, *18*(2), 144–152.

Amoon, M., Altameem, T., & Altameem, A. (2020). RRAC: Role based reputed access control method for mitigating malicious impact in intelligent IoT platforms. *Computer Communications*. https://doi.org/10.1016/j.comcom.2020.01.011

Arthur Sandor, V. K., Lin, Y., Li, X., Lin, F., & Zhang, S. (2019). Efficient decentralized multi-authority attribute based encryption for mobile cloud data storage. *Journal of Network and Computer Applications*, *129*(June 2018), 25–36. https://doi.org/10.1016/j.jnca.2019.01.003

Bakiras, S., Troja, E., & Xu, X. (2020). Secure and Anonymous Communications Over Delay Tolerant Networks. *IEEE Access*, *8*. https://doi.org/10.1109/ACCESS.2020.2993062

Baniata, H., Almobaideen, W., & Kertesz, A. (2020). A Privacy Preserving Model for Fog-enabled MCC systems using 5G Connection. *2020 5th International Conference on Fog and Mobile Edge Computing, FMEC 2020*, 223–230. https://doi.org/10.1109/FMEC49853.2020.9144814

Banks, J. (2010). *Discrete-Event System Simulation*. Prentice Hall.

Baseri, Y., Hafid, A., & Cherkaoui, S. (2016). K-anonymous Location-based Fine-grained Access Control for Mobile Cloud. In *13th IEEE Annual Consumer Communications & Networking Conference (CCNC)* (pp. 720–725). IEEE.

Baseri, Y., Hafid, A., & Cherkaoui, S. (2018). Privacy preserving fine-grained location-based access control for mobile cloud. *Computers & Security*, *73*, 249–265. https://doi.org/10.1016/j.cose.2017.10.014

Benet, J. (2014). *IPFS - Content Addressed, Versioned, P2P File System*.

Bethencourt, J., & Waters, B. (2007). Ciphertext-Policy Attribute-Based Encryption. *IEEE Computer Society*.

Bhajantri, L. B., & Mujawar, T. (2019). A Survey of Cloud Computing Security Challenges, Issues and their Countermeasures. *Proceedings of the 3rd International Conference on I-SMAC IoT in Social, Mobile, Analytics and Cloud, I-SMAC 2019*, 376–380. https://doi.org/10.1109/I-SMAC47947.2019.9032545

Bhatt, S., Antonio, S., & Antonio, S. (2017). ABAC with Group Attributes and Attribute Hierarchies Utilizing the Policy Machine. In *2nd ACM Workshop on Attribute-Based Access Control* (pp. 17–28). Scottsdale, AZ, USA: ACM.

Biswas, P., Sandhu, R., & Krishnan, R. (2017). Attribute Transformation for Attribute-Based Access Control. In *2nd ACM Workshop on Attribute-Based Access Control* (pp. 1–8). Scottsdale, AZ, USA: ACM.

Boneh, D., & Franklin, M. (2003). *Identity-Based Encryption from the Weil Pairing*. *Advances in Cryptology—CRYPTO 2001* (Vol. 32). Springer.

Borst, S., Gupta, V., Walid, A., Labs, B., Avenue, M., Box, P. O., & Hill, M. (2010). Distributed Caching Algorithms for Content Distribution Networks. In *IEEE INFOCOM* (pp. 1–9). San Diego, CA: IEEE.

Caro, A. De, & Iovino, V. (2011). Java Pairing-Based Cryptography Library(JPBC). Retrieved from http://gas.dia.unisa.it/projects/jpbc

Charanya, R., & Aramudhan, M. (2016). Survey on Access Control Issues in Cloud Computing. In *International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS)* (pp. 13–14). IEEE.

Chase, M. (2007). Multi-authority Attribute Based Encryption. In *Theory of Cryptography Conference* (pp. 515–534). Springer.

Chase, M., & Chow, S. S. M. (2009). Improving Privacy and Security in Multi-Authority Attribute-Based Encryption. In *CCS'09, November 9–13, 2009, Chicago, Illinois, USA* (pp. 121–130).

Chatterjee, S., Roy, S., Das, A. K., Chattopadhyay, S., Kumar, N., Reddy, A. G., & Member, S. (2017). On the Design of Fine Grained Access Control with User Authentication Scheme for Telecare Medicine Information Systems. *IEEEE*, *3536*(c), 1–19. https://doi.org/10.1109/ACCESS.2017.2694044

Chen, J., & Gong, J. (2018). Unbounded ABE via Bilinear Entropy Expansion , Revisited. In *EUROCRYPT* (pp. 503–534). Springer.

Chen, S.-T., Xu, J.-F., Hang, Y.-X., & Li, J. (2016). Role-based Access Control for Memory Security on Network-on-Chips. In *13th IEEE International Conference on Solid-State and Integrated Circuit Technology (ICSICT)* (pp. 3–5). IEEE. https://doi.org/10.1109/ICSICT.2016.7998757

Cisco. (2019). Cisco visual networking index (VNI) global mobile data traffic forecast update, 2017-2022 white paper. *Ca*, *Usa*, 3–5. Retrieved from http://www.gsma.com/spectrum/wp-content/uploads/2013/03/Cisco_VNI-global-mobile-data-traffic-forecast-update.pdf

Cohen, B. (2003). Incentives Build Robustness in BitTorrent. In *Workshop on Economics of Peer-to-Peer Systems* (pp. 68–72).

Comput, J. P. D., Ur, M., Guidi, B., & Baiardi, F. (2020). Blockchain-based access control management for Decentralized Online Social Networks. *Journal of Parallel and Distributed Computing*, *144*, 41–54. https://doi.org/10.1016/j.jpdc.2020.05.011

Cui, H., Deng, R. H., Lai, J., & Yi, X. (2018). An efficient and expressive ciphertext-policy attribute-based encryption scheme with partially hidden access structures. *Computer Networks*, *133*, 157–165. https://doi.org/10.1016/j.comnet.2018.01.034

Dang, N. T., Le, H. D., Le, S. T., & Tran, H. (n.d.). Applying attribute-based encryption on mobile devices, *3*.

Das, S., Sural, S., Vaidya, J., & Atluri, V. (2019). Policy adaptation in hierarchical attribute-based access control systems. *ACM Transactions on Internet Technology*, *19*(3). https://doi.org/10.1145/3323233

Denisow, I., Zickau, S., Beierle, F., & Axel, K. (2015). Dynamic Location Information in Attribute-based Encryption Schemes. In *2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies*. https://doi.org/10.1109/NGMAST.2015.63

Di, D., Maesa, F., Mori, P., Ricci, L., & Nazionale, C. (2019). A blockchain based approach for the definition of auditable Access Control systems. *Computers & Security*, *84*, 93–119. https://doi.org/10.1016/j.cose.2019.03.016

Di Pietro, R., Scarpa, M., & Puliafito, A. (2019). How Much Enhancing Confidentiality and Integrity on Data Can Affect Mobile Multi-Cloud: The "aRIANNA" Experience. *Proceedings - 2019 IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises, WETICE 2019*, 346–350. https://doi.org/10.1109/WETICE.2019.00077

Dias, J. P., Sereno Ferreira, H., & Martins, Â. (2020). A Blockchain-Based Scheme for Access Control in e-Health Scenarios. *Advances in Intelligent Systems and Computing*, *942*, 238–247. https://doi.org/10.1007/978-3-030-17065-3_24

Ding, S., Cao, J., Li, C., Fan, K., & Li, H. (2019). A Novel Attribute-Based Access Control Scheme Using Blockchain for IoT. *IEEE Access*, *7*(8), 38431–38441. https://doi.org/10.1109/ACCESS.2019.2905846

Dinh, T. T. A., Wang, J., Chen, G., Liu, R., & Ooi, C. (2017). BLOCKBENCH : A Framework for Analyzing Private. In *ACM International Conference on Management of Data (SIGMOD '17)*, (pp. 1085–1100). New York, NY, USA: ACM.

Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017). Blockchain for IoT Security and Privacy : The Case Study of a Smart Home. In *2ND IEEE PERCOM Workshop On Security Privacy And Trust In The Internet of Things 2017* (pp. 618–623). IEEE.

El Sibai, R., Gemayel, N., Bou Abdo, J., & Demerjian, J. (2020). A survey on access control mechanisms for cloud computing. *Transactions on Emerging Telecommunications Technologies*, *31*(2), 1–21. https://doi.org/10.1002/ett.3720

Elliott, A., & Knight, S. (2016). Start Here : Engineering Scalable Access Control Systems. In *21st ACM on Symposium on Access Control Models and Technologies* (pp. 113–124). ACM.

Eltayieb, N., Wang, P., Hassan, A., Elhabob, R., & Li, F. (2019). ASDS: Attribute-based secure data sharing scheme for reliable cloud environment. *Security and Privacy*, *2*(2), e57. https://doi.org/10.1002/spy2.57

Ezhilarasan, E., & Dinakaran, M. (2021). Privacy preserving and data transpiration in multiple cloud using secure and robust data access management algorithm. *Microprocessors and Microsystems*, *82*(January), 103956. https://doi.org/10.1016/j.micpro.2021.103956

Fadhel, A. Ben, Bianculli, D., & Briand, L. C. (2018). Model-driven run-time enforcement of complex role-based access control policies. *ASE 2018 - Proceedings of the 33rd ACM/IEEE International Conference on Automated Software Engineering*, 248–258. https://doi.org/10.1145/3238147.3238167

Fakhfakh, F. (2019). Performance and correctness of mobile cloud computing systems: Taxonomy and open challenges. *2019 15th International Wireless Communications and Mobile Computing Conference, IWCMC 2019*, 1019–1024. https://doi.org/10.1109/IWCMC.2019.8766588

Fan, Y., Liu, S., Tan, G., & Qiao, F. (2020). Fine-grained access control based on Trusted Execution Environment. *Future Generation Computer Systems*, *109*, 551–561. https://doi.org/10.1016/j.future.2018.05.062

Fang, C., Yu, F. R., Huang, T., Liu, J., & Liu, Y. (2014). A Survey of Energy-Efficient Caching in Information-Centric Networking. *Green Communications and Computing Networks*, (November), 122–129.

Farooq, M. U., Waseem, M., Khairi, A., & Sadia Mazhar. (2015). A Critical Analysis on the Security Concerns of Internet of Things (IoT). *International Journal OfComputer Applications*, *111*(7), 1–6.

Freeman, D. M. (2010). Converting Pairing-Based Cryptosystems from Composite-Order Groups to Prime-Order Groups. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques* (pp. 44–61).

Fu, X., Nie, X., Wu, T., & Li, F. (2018). Large universe attribute based access control with efficient decryption in cloud storage system. *The Journal of Systems and Software*, *135*(January), 157–164. https://doi.org/10.1016/j.jss.2017.10.020

Fugkeaw, S. (2021). A Fine-Grained and Lightweight Data Access Control Model for Mobile Cloud Computing. *IEEE Access*, *9*, 836–848. https://doi.org/10.1109/ACCESS.2020.3046869

Gai, K., Qiu, L., Chen, M., Zhao, H., & Qiu, M. (2017). Sa-East : Security-Aware Efficient Data Transmission for ITS in Mobile Heterogeneous Cloud Computing. *ACM Transactions on Embedded Computing Systems*, *16*(2), 1–22. https://doi.org/10.1145/2979677

Gai, K., Qiu, M., & Elnagdy, S. A. (2016). Security-Aware Information Classifications Using Supervised Learning for Cloud-Based Cyber Risk Management in Financial Big Data. *Proceedings - 2nd IEEE International Conference on Big Data Security on Cloud*, 197–202. https://doi.org/10.1109/BigDataSecurity-HPSC-IDS.2016.66

Gai, K., Qiu, M., Zhao, H., & Dai, W. (2016). Privacy-Preserving Adaptive Multi-channel Communications under Timing Constraints. *Proceedings - 2016 IEEE International Conference on Smart Cloud, SmartCloud 2016*, 190–195. https://doi.org/10.1109/SmartCloud.2016.50

Galeano-Brajones, J., Carmona-Murillo, J., Luna-Valero, F., & Valenzuela-Valdés, J. F. (2020). Detection and Mitigation of DoS and DDoS Attacks in IoT-Based Stateful SDN : An Experimental Approach. *Sensors*, *20*(3). https://doi.org/10.3390/s20030816

Ge, C., Susilo, W., Wang, J., Shi, Y., & Fang, L. (2018). A CCA-secure key-policy attribute-based proxy re-encryption in the adaptive corruption model for dropbox data sharing system. *Designs, Codes and Cryptography*, *86*(11), 2587–2603. https://doi.org/10.1007/s10623-018-0462-9

Goyal, V., Jain, A., Pandey, O., & Sahai, A. (2008). Bounded Ciphertext Policy Attribute Based Encryption - Semantic Scholar. *International Colloquium on Automata, Languages, and Programming*, 579–591. Retrieved from https://www.semanticscholar.org/paper/Bounded-Ciphertext-Policy-Attribute-Based-Goyal-Jain/4db8718a0043cf0f50cc0df6a5fbc534a302ca14

Goyal, V., Pandey, O., Sahai, A., Waters, B., Pandey, O., Sahai, A., & Waters, B. (2006). Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data. In *CCS '06: Proceedings of the 13th ACM conference on Computer and communications security* (pp. 89–98). ACM.

Goyal, V., & Waters, B. (2006). Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data. In *Proceedings of the 13th ACM conference on Computer and communications security* (pp. 89–98). ACM.

Gu, J., Wang, W., Huang, A., Shan, H., & Zhang, Z. (2014). Distributed Cache Replacement for Caching-Enable Base Stations in Cellular Networks. In *International Conference on Communications (ICC)* (pp. 2648–2653). Sydney, NSW: IEEE.

Guo, L., Yang, X., & Yau, W. C. (2021). TABE-DAC: Efficient Traceable Attribute-Based Encryption Scheme with Dynamic Access Control Based on Blockchain. *IEEE Access*, *9*, 8479–8490. https://doi.org/10.1109/ACCESS.2021.3049549

Han, J., Susilo, W., Mu, Y., Zhou, J., & Au, M. H. (2014). Improving Privacy and Security in Decentralized Ciphertext-Policy Attribute-Based Encryption. *IEEE Transactions on Information Forensics and Security*, *6013*, 665–678. https://doi.org/10.1109/TIFS.2014.2382297

Han, Q., Zhang, Y., & Li, H. (2018). Efficient and Robust Attribute-based Encryption Supporting Access Policy Hiding in Internet of Things. *Future Generation Computer Systems*, *83*(June), 269–277. https://doi.org/10.1016/j.future.2018.01.019

Hao, J., Liu, J., Wang, H., Liu, L., Xian, M., & Shen, X. (2019). Efficient Attribute-Based Access Control with Authorized Search in Cloud Storage. *IEEE Access*, *7*, 182772–182783. https://doi.org/10.1109/ACCESS.2019.2906726

Herranz, J., Laguillaumie, F., & Carla, R. (2010). Constant Size Ciphertexts in Threshold Attribute-Based Encryption. *Proceedings Oft He International Workshop on Public Key Cryptography (PKC'10)*, *6056*, 19–34.

Herrmann, D. S. (2002). *A Practical Guide to Security Engineering and Information Assurance*. AUERBACH PUBLICATIONS.

Herrmann, D. S. (2007). *Complete Guiese to Security And Privacy Metrics*. (T. & F. Group, Ed.). AUERBACH PUBLICATIONS.

Hong, H., & Sun, Z. (2016). High efficient key - insulated attribute based encryption scheme without bilinear pairing operations. *SpringerPlus*, *5*(1), 131. https://doi.org/10.1186/s40064-016-1765-9

Hossain, M., Fotouhi, M., & Hasan, R. (2015). Towards an Analysis of Security Issues , Challenges , and Open Problems in the Internet of Things. In *2015 IEEE World Congress on Services* (pp. 21–28). IEEE. https://doi.org/10.1109/SERVICES.2015.12

Hossain, M. J., Xu, C., & Li, C. (2020). A Secure Authentication Scheme for Mobile Cloud Computing against CCA. *2020 17th International Computer Conference on Wavelet Active Media Technology and Information Processing, ICCWAMTIP 2020*, 266–270. https://doi.org/10.1109/ICCWAMTIP51612.2020.9317383

Hu, V. C., Kuhn, D. R., & Ferraiolo, D. F. (2015). Attribute-Based Access Control. *IEEE Computer Society*, (February), 85–88.

Huang, D., Dong, Q., & Zhu, Y. (2020). *Attribute Based Encryption and Access Control*. Taylor & Francis.

Huang, H., Lin, J., & Zheng, B. (2020). When Blockchain Meets Distributed File Systems : An Overview , Challenges , and Open Issues. *IEEE Access*, *8*, 50574–50586. https://doi.org/10.1109/ACCESS.2020.2979881

Hurtuk, J., Baláž, A., & Ádám, N. (2016). Security Sandbox Based on RBAC Model. In *11th IEEE International Symposium on Applied Computational Intelligence and Informatics* (pp. 75–80). Timişoara, Romania: IEEE.

Ibrahim, I. M., Mostafa, M. G. M., Hazem, S., El-Gohary, R., & Faheem, H. M. (2018). A Robust Generic Multi-Authority Attributes Management System for Cloud Storage Services. *IEEE Transactions on Cloud Computing*, *9*(2), 435–446. https://doi.org/10.1109/TCC.2018.2867871

Ioannou, A., & Weber, S. (2016). A Survey of Caching Policies and Forwarding Mechanisms in Information-Centric Networking. *IEEE Communications Surveys & Tutorials*, *18*(4), 2847–2886.

Irshad, A., Chaudhry, S. A., Shafiq, M., Usman, M., Asif, M., & Ghani, A. (2019). A provable and secure mobile user authentication scheme for mobile cloud computing services. *International Journal of Communication Systems*, *32*(14), 1–19. https://doi.org/10.1002/dac.3980

Jahid, S., Mittal, P., & Borisov, N. (2011). EASiER : Encryption-based Access Control in Social Networks with Efficient Revocation. In *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security* (pp. 411–415).

Jemel, M., & Serhrouchni, A. (2017). Decentralized access control mechanism with temporal dimension based on blockchain. In *The Fourteenth IEEE International Conference on e-Business Engineering* (pp. 177–182). Shanghai, China: IEEE. https://doi.org/10.1109/ICEBE.2017.35

Jiang, W., Feng, G., & Qin, S. (2016). Optimal Cooperative Content Caching and Delivery Policy for Heterogeneous Cellular Networks. *IEEE Transactions on Mobile Computing*, 1–13. https://doi.org/10.1109/TMC.2016.2597851

Jiguo, L., Qihong, Y., & Yichen, Z. (2019). Hierarchical attribute based encryption with continuous leakage-resilience. *Information Sciences*, *484*, 113–134. https://doi.org/10.1016/j.ins.2019.01.052

Junwei, W. (2012). Java realization for Ciphertext- Policy Attribute-Based Encryption. Retrieved from https://github.com/junwei-wang/cpabe/

Kalinin, M., Krundyshev, V., Rezedinova, E., & Zegzhda, P. (2018). Role-Based Access Control for Vehicular Adhoc Networks. *2018 IEEE International Black Sea Conference on Communications and Networking, BlackSeaCom 2018*. https://doi.org/10.1109/BlackSeaCom.2018.8433628

Karatas, G., & Akbulut, A. (2018). Survey on Access Control Mechanisms in Cloud Computing. *Journal of Cyber Security and Mobility*, *7*, 1–36. https://doi.org/10.13052/jcsm2245-1439.731

Karati, A., & Amin, R. (2016). Provably Secure Threshold-Based ABE Scheme Without Bilinear Map. *Arabian Journal for Science and Engineering*, *41*(8), 3201–3213. https://doi.org/10.1007/s13369-016-2156-9

Karimi, L., Aldairi, M., Joshi, J., & Abdelhakim, M. (2021). An Automatic Attribute Based Access Control Policy Extraction from Access Logs. *IEEE Transactions on Dependable and Secure Computing*, *5971*(c), 1–14. https://doi.org/10.1109/TDSC.2021.3054331

Kerr, L., & Alves-foss, J. (2016). Combining Mandatory and Attribute-based Access Control. In *49th Hawaii International Conference on System Sciences* (pp. 2616–2623). IEEE. https://doi.org/10.1109/HICSS.2016.328

Khan, A. Y. A. R., Latif, R., & Latif, S. (2020). Malicious Insider Attack Detection in IoTs Using Data Analytics. *IEEE Access*, *8*, 11743–11753.

Khan, F., Li, H., & Zhang, L. (2016). Owner Specified Excessive Access Control for Attribute Based Encryption. *IEEE Access*, *4*(November), 967–8976. https://doi.org/10.1109/ACCESS.2016.2632132

Khan, M. F. F., & Sakamura, K. (2015). Fine-Grained Access Control to Medical Records in Digital Healthcare Enterprises. In *International Symposium on, Networks, Computers and Communications (ISNCC)* (pp. 1–6). IEEE.

Ko, J. Y., Lee, S. G., & Lee, C. H. (2019). Real-time Mandatory Access Control on SELinux for Internet of Things. In *2019 IEEE International Conference on Consumer Electronics, ICCE 2019*. IEEE. https://doi.org/10.1109/ICCE.2019.8662112

Koblitz, B. N. (1987). Elliptic Curve Cryptosystems. *Mathematic of Computation*, *4*(177), 203–209.

Koblitz, N., Menezes, A., & Vanstone, S. (2000). *The State of Elliptic Curve Cryptography* (Vol. 193).

Kumar, K. D., & Reddy, D. A. K. (2014). Concrete Attribute-Based Encryption Scheme with Verifiable Outsourced Decryption. *International Journal of Engineering Trends and Technology (IJETT)*, *12*(9), 421–426.

Kumar, R. (2020). A Systematic Review of the Security in Cloud Computing : Data Integrity , Confidentiality and Availability. In *2020 IEEE International Conference on Computing, Power and Communication Technologies (GUCON) Galgotias University, Greater Noida, UP, India. Oct 2-4, 2020* (pp. 334–337).

Labs, P. (2017). *Filecoin : A Decentralized Storage Network*.

Laverdière, M.-A., Julien, K., & Merlo, E. (2021). RBAC protection-impacting changes identification: A case study of the security evolution of two PHP applications. *Information and Software Technology*, 106630. https://doi.org/10.1016/j.infsof.2021.106630

Law, A. M. (2003). HOW TO CONDUCT A SUCCESSFUL SIMULATION STUDY. In *2003 Winter Simulation Conference* (pp. 66–70).

Lee, K. (2020). Revocable Hierarchical Identity-Based Encryption with Adaptive Security. *Theoretical Computer Science*. https://doi.org/10.1016/j.tcs.2021.05.034

Lenstra, B. H. W. (1987). Factoring integers with elliptic curves. *Annals of Mathematics*, *126*, 649–673.

Lewko, A., Okamoto, T., Sahai, A., Takashima, K., & Waters, B. (2010). Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *6110 LNCS*(subaward 641), 62–91. https://doi.org/10.1007/978-3-642-13190-5_4

Lewko, A., & Waters, B. (2011). Decentralizing Attribute-Based Encryption. In K. G. Paterson (Ed.), *Annual international conference on the theory and applications of cryptographic techniques* (Vol. 02, pp. 568–588). Berlin, Heidelberg: Springer.

Lewko, A., & Waters, B. (2012). New proof methods for attribute-based encryption: Achieving full security through selective techniques. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *7417 LNCS*, 180–198. https://doi.org/10.1007/978-3-642-32009-5_12

Li, F., Rahulamathavan, Y., Conti, M., & Rajarajan, M. (2015). Robust access control framework for mobile cloud computing network. *Comput. Commun.*, *68*(C), 61–72. https://doi.org/10.1016/j.comcom.2015.07.005

Li, Jiguo, Lin, X., Zhang, Y., & Han, J. (2016). KSF-OABE : Outsourced Attribute-Based Encryption with Keyword Search Function for Cloud Storage. *IEEE Transactions on Services Computing*, *1374*, 1–12. https://doi.org/10.1109/TSC.2016.2542813

Li, Jiguo, Yao, W., Han, J., Zhang, Y., & Shen, J. (2017). User Collusion Avoidance CP-ABE With Efficient Attribute Revocation for Cloud Storage. *IEEE Systems Journal*, *12*(2), 1767–1777.

Li, Jiguo, Yu, Q., Zhang, Y., & Shen, J. (2018). Key-Policy Attribute-Based Encryption against Continual Auxiliary Input Leakage. *Information Sciences*, 175–188. https://doi.org/10.1016/j.ins.2018.07.077

Li, Jiguo, Zhang, Y., Ning, J., Huang, X., Poh, G. Sen, & Wang, D. (2020). Attribute Based Encryption with Privacy Protection and Accountability for CloudIoT. *IEEE Transactions on Cloud Computing*, *7161*(c), 1–1. https://doi.org/10.1109/tcc.2020.2975184

Li, Jin, Chen, X., Chow, S. S. M., Huang, Q., Wong, D. S., & Liu, Z. (2018). Multi-authority fine-grained access control with accountability and its application in cloud. *Journal of Network and Computer Applications*. https://doi.org/10.1016/j.jnca.2018.03.006

Li, Jin, Ye, H., Li, T., Wang, W., Lou, W., Hou, T., … Lu, R. (2020). Efficient and Secure Outsourcing of Differentially Private Data Publishing with Multiple Evaluators. *IEEE Transactions on Dependable and Secure Computing*, *5971*(c), 1–11. https://doi.org/10.1109/TDSC.2020.3015886

Li, Jin, Zhang, Y., Chen, X., & Xiang, Y. (2017). Secure Attribute-Based Data Sharing for Resource-Limited Users in Cloud Computing. *Computers & Security*, *72*(January 2018), 1–12. https://doi.org/10.1016/j.cose.2017.08.007

Li, R., Song, T., Mei, B., Li, H., Cheng, X., Sun, L., … Worth, F. (2020). Blockchain For Large-Scale Internet of Things Data Storage and Protection. *IEEE Transactions on Services Computing*, *1374*, 99. https://doi.org/10.1109/TSC.2018.2853167

Li, W. M., Li, X. L., Wen, Q. Y., Zhang, S., & Zhang, H. (2017). Flexible CP-ABE Based Access Control on Encrypted Data for Mobile Users in Hybrid Cloud System. *Journal of Computer Science and Technology*, *32*(5), 974–990. https://doi.org/10.1007/s11390-017-1776-1

Li, Y., Dai, W., Ming, Z., & Qiu, M. (2016). Privacy Protection for Preventing Data Over-Collection in Smart City. *IEEE Transactions on Computers*, *65*(5), 1339–1350. https://doi.org/10.1109/TC.2015.2470247

Liang, X., Cao, Z., Xing, D., & Lin, H. (2009). Provably Secure and Efficient Bounded Ciphertext Policy Attribute Based Encryption Categories and Subject Descriptors. In *ASIACCS '09, March 10-12, 2009, Sydney, NSW, Australia.* (pp. 343–352).

Liao, B., Ali, Y., Nazir, S., He, L., & Khan, H. U. (2020). Security Analysis of IoT Devices by Using Mobile Computing: A Systematic Literature Review. *IEEE Access*, *8*, 120331–120350. https://doi.org/10.1109/ACCESS.2020.3006358

Lin, G., Hong, H., & Sun, Z. (2017). A Collaborative Key Management Protocol in Ciphertext Policy Attribute-Based Encryption for Cloud Data Sharing. *IEEE Access*, *5*, 9464–9475. https://doi.org/10.1109/ACCESS.2017.2707126

Ling, J., & Weng, A. X. (2018). A scheme of hidden-structure attribute-based encryption with multiple authorities. In *IOP Conference Series: Materials Science and Engineering* (p. 012005). https://doi.org/10.1088/1757-899X/359/1/012005

Liu, B., Yu, X. L., Chen, S., Xu, X., & Zhu, L. (2017). Blockchain based Data Integrity Service Framework for IoT data. In *24th International Conference on Web Services* (pp. 468–475). Honolulu, HI, USA: IEEE. https://doi.org/10.1109/ICWS.2017.54

Liu, C., Hsien, W., Yang, C., & Hwang, M. (2016). A Survey of Attribute-based Access Control with User Revocation in Cloud Data Storage. *International Journal of Network Security*, *18*(5), 900–916.

Liu, Y., Zhang, Y., Ling, J., & Liu, Z. (2018). Secure and fine-grained access control on e-healthcare records in mobile cloud computing. *Future Generation Computer Systems*, *78*(January 2018), 1020–1026. https://doi.org/10.1016/j.future.2016.12.027

Liu, Z., Jiang, Z. L., Wang, X., & Yiu, S. M. (2018). Practical attribute-based encryption : Outsourcing decryption , attribute revocation and policy updating. *Journal of Network and Computer Applications*, *108*(February), 112–123. https://doi.org/10.1016/j.jnca.2018.01.016

Lynn, B. (2007). *ON THE IMPLEMENTATION OF PAIRING-BASED CRYPTOSYSTEMS*.

Madine, M. M., Battah, A. A., Yaqoob, I., Salah, K., Jayaraman, R., Al-Hammadi, Y., … Ellahham, S. (2020). Blockchain for Giving Patients Control over Their Medical Records. *IEEE Access*, *8*, 193102–193115. https://doi.org/10.1109/ACCESS.2020.3032553

Mahmoodi, S. E., Uma, R. N., & Subbalakshmi, K. P. (2019). Optimal joint scheduling and cloud offloading for mobile applications. *IEEE Transactions on Cloud Computing*, *7*(2), 301–313. https://doi.org/10.1109/TCC.2016.2560808

Malluhi, Q. M., Shikfa, A., & Trinh, V. C. (2017). A ciphertext-policy attribute-based encryption scheme with optimized ciphertext size and fast decryption. *ASIA CCS 2017 - Proceedings of the 2017 ACM Asia Conference on Computer and Communications Security*, 230–240. https://doi.org/10.1145/3052973.3052987

Mamta, & Gupta, B. B. (2019). An efficient KP design framework of attribute-based searchable encryption for user level revocation in cloud. *Concurrency Computation* , (February 2019), 1–17. https://doi.org/10.1002/cpe.5291

Maymounkov, P., & Mazires, D. (2002). Kademlia: A Peer-to-peer Information System Based on the XOR Metric. In *International Workshop on Peer-to-Peer Systems* (pp. 53–65). Springer.

Mazieres, D. (2000). *Self-certifying File System*. MASSACHUSETTS INSTITUTE OF TECHNOLOGY.

Merdassi, I., Ghazel, C., & Saidane, L. (2020). Surveying and analyzing security issues in mobile cloud computing. *2020 9th IFIP International Conference on Performance Evaluation and Modeling in Wireless Networks, PEMWN 2020*. https://doi.org/10.23919/PEMWN50727.2020.9293077

Miao, Y., Liu, X., Choo, K. R., Member, S., Deng, H., Li, J., … Ma, J. (2019). Privacy-Preserving Attribute-Based Keyword Search in Shared Multi-owner Setting. *IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING*, 1–15.

Miao, Y., Ma, J., Liu, X., Zhang, J., & Liu, Z. (2017). VKSE-MO: verifiable keyword search over encrypted data in multi-owner settings. *Science China Information Sciences*, *60*(12), 1–15. https://doi.org/10.1007/s11432-016-0540-x

Michalevsky, Y., & Joye, M. (2018). Decentralized Policy-Hiding Attribute-Based Encryption with Receiver Privacy. In *IACR Cryptology* (pp. 1–29).

Miller, V. S. (1985). Use of Elliptic Curves in Cryptography. In *Theory and Application of Cryptographic Techniques CRYPTO 1985* (pp. 417–426).

Mitra, B., Sural, S., Vaidya, J., & Atluri, V. (2017). Migrating from RBAC to temporal RBAC. *IET Information Security*, *11*(5), 294–300. https://doi.org/10.1049/iet-ifs.2016.0258

Msahli, M., Chen, X., & Serhrouchni, A. (2014). Towards a fine-grained access control for Cloud. In *2014 IEEE 11th International Conference on e-Business Engineering Towards* (pp. 286–291). IEEE. https://doi.org/10.1109/ICEBE.2014.56

Murugaanandam, S., Pandey, V., & Tiwari, S. (2020). PRIVACY PROTECTION OVER CLOUD USING AES ENCRYPTION. *European Journal of Molecular & Clinical Medicine*, *7*(10), 1980–1990.

Newport, C. (2007). Provably Secure Ciphertext Policy ABE Categories and Subject Descriptors, 456–465.

Ning, J., & Kim-Kwang Raymond Choo. (2018). CryptCloud + : Secure and Expressive Data Access Control for Cloud Storage. *IEEE Transactions on Services Computing*, (October). https://doi.org/10.1109/TSC.2018.2791538

Noor, T. H., Zeadally, S., Alfazi, A., & Sheng, Q. Z. (2018). Journal of Network and Computer Applications Mobile cloud computing : Challenges and future research directions. *Journal of Network and Computer Applications*, *115*(May), 70–85. https://doi.org/10.1016/j.jnca.2018.04.018

Odelu, V., Das, A. K., Rao, Y. S., Kumari, S., Khan, M. K., & Choo, K. R. (2016). Pairing-based CP-ABE with constant-size ciphertexts and secret keys for cloud environment. *Computer Standards & Interfaces*, *54*(September), 3–9. https://doi.org/10.1016/j.csi.2016.05.002

Ogwara, N. O., Petrova, K., & Yang, M. L. B. (2019). Data Security Frameworks for Mobile Cloud Computing: A Comprehensive Review of the Literature. *2019 29th International Telecommunication Networks and Applications Conference, ITNAC 2019*, 2019–2022. https://doi.org/10.1109/ITNAC46935.2019.9078007

Ohtake, G., Safavi-Naini, R., & Zhang, L. F. (2017). Outsourcing scheme of ABE encryption secure against malicious adversary. *ICISSP 2017 - Proceedings of the 3rd International Conference on Information Systems Security and Privacy*. https://doi.org/10.5220/0006129600710082

Omar, I. A., Jayaraman, R., Salah, K., Simsekler, M. C. E., Yaqoob, I., & Ellahham, S. (2020). Ensuring protocol compliance and data transparency in clinical trials using Blockchain smart contracts. *BMC Medical Research Methodology*, *20*(1), 1–17. https://doi.org/10.1186/s12874-020-01109-5

Pareek, G., & Purushothama, B. R. (2020). Proxy re-encryption for fine-grained access control: Its applicability, security under stronger notions and performance. *Journal of Information Security and Applications*, *54*. https://doi.org/10.1016/j.jisa.2020.102543

Patil, R. G. M., & Dhananjaya, V. (2018). Cloud ++ : A Secure and Timed Data Access Control Scheme for Cloud. *International Journal of Innovative Research in Science, Engineering and Technology*, *7*(6), 90–95.

Patsakis, C., & Casino, F. (2019). Hydras and IPFS : A Decentralised Playground for Malware. *Int. J. Inf. Secur [8]*, *8*, 1–22.

Phillips, T., Yu, X., Haakenson, B., & Zou, X. (2019). Design and implementation of privacy-preserving, flexible and scalable role-based hierarchical access control. *Proceedings - 1st IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications, TPS-ISA 2019*, 46–55. https://doi.org/10.1109/TPS-ISA48467.2019.00015

Podlipning, S., & Boszormenyi, L. (2014). A survey of Web cache replacement strategies. *ACM Computing Surveys (CSUR)*, *35*(May), 374–398. https://doi.org/10.1145/954339.954341

Politou, E., Alepis, E., Patsakis, C., & Casino, F. (2020). Delegated content erasure in IPFS. *Future Generation Computer Systems*, *112*, 956–964. https://doi.org/10.1016/j.future.2020.06.037

Politou, E., Casino, F., Alepis, E., & Patsakis, C. (2019). Blockchain Mutability : Challenges and Proposed Solutions. *IEEE TRANSACTIONS ON EMERGING TOPICS IN COMPUTING*, *6750*(MARCH), 1. https://doi.org/10.1109/TETC.2019.2949510

Pooryousef, S., & Amini, M. (2016). Fine-Grained Access Control for Hybrid Mobile Applications in Android Using Restricted Paths. In *13th International Iranian Society of Cryptology Conference on Information Security and Cryptology (ISCISC)* (pp. 85–90).

Qi, H., Di, X., & Li, J. (2018). Formal definition and analysis of access control model based on role and attribute. *Journal of Information Security and Applications*, *43*, 53–60. https://doi.org/10.1016/j.jisa.2018.09.001

Qi, Q., Liao, J., Wang, J., Li, Q., & Cao, Y. (2016). Dynamic resource orchestration for multi-task application in heterogeneous mobile cloud computing. *Proceedings - IEEE INFOCOM*, *2016-Septe*(1), 221–226. https://doi.org/10.1109/INFCOMW.2016.7562076

Qiu, M., & Gai, K. (2017). *Mobile cloud computing: Models, implementation, and security*. *Mobile Cloud Computing: Models, Implementation, and Security*. https://doi.org/10.1201/b21556

Rahulamathavan, Y., Phan, R. C., Rajarajan, M., Misra, S., & Kondoz, A. (2017). Privacy-preserving Blockchain based IoT Ecosystem using Attribute-based Encryption. In *International Conference on Advanced Networks and Telecommunications Systems (ANTS)* (pp. 1–6). IEEE.

Ramos, R. M., Martinello, M., & Esteve Rothenberg, C. (2013). SlickFlow: Resilient source routing in data center networks unlocked by OpenFlow. *Proceedings - Conference on Local Computer Networks, LCN*, 606–613. https://doi.org/10.1109/LCN.2013.6761297

Rana, K., Yadav, H., & Agrawal, C. (2020). Mutual Authentication and Location Privacy using HECC and SHA 2 in Mobile Cloud Computing Environment. *2020 6th International Conference on Advanced Computing and Communication Systems, ICACCS 2020*, 362–369. https://doi.org/10.1109/ICACCS48705.2020.9074369

Rauf, A., Abdullah, A. H., Iqbal, S., & Awan, K. (2019). Perception Reasoning Task-Role RBAC for Data Access Control in Cloud. *International Journal of Computing & Communication Networks*, *1*(1), 1–9.

Rizvi, S., Kurtz, A., Pfeffer, J., & Rizvi, M. (2018). Securing the Internet of Things (IoT): A Security Taxonomy for IoT. In *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)* (pp. 163–168). IEEE. https://doi.org/10.1109/TrustCom/BigDataSE.2018.00034

Roman, R., Lopez, J., & Mambo, M. (2018). Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges. *Future Generation Computer Systems*, *78*, 680–698. https://doi.org/10.1016/j.future.2016.11.009

Rouselakis, Y., & Waters, B. (2013). Practical constructions and new proof methods for large universe attribute-based encryption. *Proceedings of the ACM Conference on Computer and Communications Security*, 463–474. https://doi.org/10.1145/2508859.2516672

Rouselakis, Y., & Waters, B. (2015). Efficient Statically-Secure Large-Universe Multi-Authority Attribute-Based Encryption. In *International Conference on Financial Cryptography and Data Security* (pp. 315–332).

Ruj, S., Nayak, A., & Stojmenovic, I. (2011). DACC : Distributed Access Control in Clouds. In *Trust, Security and Privacy in Computing and Communications (TrustCom), 2011 IEEE 10th International Conference* (pp. 91–98). IEEE. https://doi.org/10.1109/TrustCom.2011.15

Saberi, F., & Azmi, R. (2020). Improving offloading in mobile cloud computing. *2020 10h International Conference on Computer and Knowledge Engineering, ICCKE 2020*, 469–474. https://doi.org/10.1109/ICCKE50421.2020.9303659

Saenko, I., & Kotenko, I. (2017). Administrating Role-Based Access Control by Genetic Algorithms. In *Genetic and Evolutionary Computation Conference Companion* (pp. 1463–1470). https://doi.org/10.1145/3067695.3082509

Saffaf, M. N. (2018). *BLOCKCHAIN: ANALYSIS, COMPARISON AND CRITIQUES*. University of VAASA.

Sahai, A., & Waters, B. (2005). Fuzzy Identity-Based Encryption. In R. Cramer (Ed.), *Advances in Cryptology -- EUROCRYPT 2005* (pp. 457–473). Berlin, Heidelberg: Springer Berlin Heidelberg.

Salman, T., Zolanvari, M., Erbad, A., Jain, R., & Samaka, M. (2019). Security Services Using Blockchains : A State of the Art Survey. *IEEE Communications Surveys & Tutorials*, *21*(1), 1. https://doi.org/10.1109/COMST.2018.2863956

Saravanan, N., & Umamakeswari, A. (2021). Lattice based access control for protecting user data in cloud environments with hybrid security. *Computers and Security*, *100*, 102074. https://doi.org/10.1016/j.cose.2020.102074

Sarhan, A. Y., & Carr, S. (2017). A Highly-Secure Self-Protection Data Scheme in Clouds Using Active Data Bundles and Agent-Based Secure Multi-Party Computation. In *4th International Conference on Cyber Security and Cloud Computing* (pp. 228–236). IEEE. https://doi.org/10.1109/CSCloud.2017.36

Sascha, M., Katzenbeisser, S., & Eckert, C. (2009). Distributed Attribute-Based Encryption. In *International Conference on Information Security and Cryptology* (pp. 20–36). Springer.

Satyanarayanan, M. (2011). Mobile Computing : the Next Decade. *ACM SIG- MOBILE Mobile Computing and Communications Review*, *15*(2), 2–10.

Sayadi, S., Rejeb, S. Ben, & CHOUKAIR, Z. (2018). Blockchain Challenges and Security Schemes : A Survey. In *2018 Seventh International Conference on Communications and Networking (ComNet)*. Hammamet, Tunisia, Tunisia: IEEE. https://doi.org/10.1109/COMNET.2018.8621944

Scherer, M. (2017). *Performance and Scalability of Blockchain Networks and Smart Contracts*.

Sengupta, A., Amuru, S., Tandon, R., Buehrer, R. M., & Clancy, T. C. (2014). Learning Distributed Caching Strategies in Small Cell Networks. In *11th International Symposium on Wireless Communications Systems (ISWCS)* (pp. 917–921). Barcelona.

Sergeev, A., & Matulevicius, R. (2017). An Approach to Capture Role-Based Access Control Models from Spring Web Applications. In *2017 IEEE 21st International Enterprise Distributed Object Computing Conference*. IEEE. https://doi.org/10.1109/EDOC.2017.29

Servos, D., & Osborn, S. L. (2017). Current Research and Open Problems in Attribute-Based Access Control. *ACM Computing Surveys*, *49*(4), 65.

Shahid, M. A., Islam, N., Alam, M. M., Mazliham, M. S., & Musa, S. (2021). Towards Resilient Method: An exhaustive survey of fault tolerance methods in the cloud computing environment. *Computer Science Review*, *40*, 100398. https://doi.org/10.1016/j.cosrev.2021.100398

Shamir, A. (1984). Identity-based Cryptosystems and Signature Scheme. In *CRYPTO 84 on Advances in Cryptology* (pp. 47–53). Springer.

Shan, X., You, L., & Hu, G. (2021). Two efficient constructions for biometric-based signature in identity-based setting using bilinear pairings. *IEEE Access*, *9*, 25973–25983. https://doi.org/10.1109/ACCESS.2021.3057064

Sharma, A. (2020). Mission swachhta. *2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, 133–138.

Singh, S., Chiu, Y. C., Tsai, Y. H., & Yang, J. S. (2017). Mobile Edge Fog Computing in 5G Era: Architecture and Implementation. *Proceedings - 2016 International Computer Symposium, ICS 2016*, 731–735. https://doi.org/10.1109/ICS.2016.0151

Soni, K., & Kumar, S. (2019). Comparison of RBAC and ABAC Security Models for Private Cloud. *Proceedings of the International Conference on Machine Learning, Big Data, Cloud and Parallel Computing: Trends, Prespectives and Prospects, COMITCon 2019*, 584–587. https://doi.org/10.1109/COMITCon.2019.8862220

Stoneburner, G., Goguen, A., & Feringa, A. (2002). *Risk Management Guide for Information Technology Systems Recommendations of the National Institute of Standards and Technology*.

Sukhodolskiy, I., & Zapechnikov, S. (2018). A Blockchain-Based Access Control System for Cloud Storage. In *2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)* (pp. 1575–1578).

Sun, P. J. (2019). Privacy Protection and Data Security in Cloud Computing: A Survey, Challenges, and Solutions. *IEEE Access*, *7*, 147420–147452. https://doi.org/10.1109/ACCESS.2019.2946185

Sun, P. J. (2020). Security and privacy protection in cloud computing: Discussions and challenges. *Journal of Network and Computer Applications*. https://doi.org/10.1016/j.jnca.2020.102642

Susilo, W., Yang, G., Guo, F., & Huang, Q. (2018). Constant-size ciphertexts in threshold attribute-based encryption without dummy attributes. *Information Sciences*, *429*, 349–360. https://doi.org/10.1016/j.ins.2017.11.037

Syed, P. S., Khatri-valmik, N., & Supriya Salve, M. (2018). Introduction to Cloud Computing. *International Research Journal of Engineering and Technology (IRJET)*, *5*(2), 5–8.

Tang, Q., & Ji, D. (2010). Verifiable attribute based encryption. *International Journal of Network Security*, *10*(2), 114–120.

Tanwar, S., Parekh, K., & Evans, R. (2020). Blockchain-based electronic healthcare record system for healthcare 4.0 applications. *Journal of Information Security and Applications*, *50*, 102407. https://doi.org/10.1016/j.jisa.2019.102407

Taubmann, B., Rakotondravony, N., & Reiser, H. P. (2016). CloudPhylactor : Harnessing Mandatory Access Control for Virtual Machine Introspection in Cloud Data Centers. In *IEEE TrustCom/BigDataSE/ISPA* (pp. 957–964). IEEE. https://doi.org/10.1109/TrustCom.2016.160

Tawalbeh, L., Haddad, Y., Khamis, O., Benkhelifa, E., Jararweh, Y., & Aldosari, F. (2016). Efficient and secure software-defined mobile cloud computing infrastructure. *International Journal High Performance Computing and Networking*, *9*(4), 328–341.

Tissir, N., El Kafhali, S., & Aboutabit, N. (2020). Cloud Computing security classifications and taxonomies: A comprehensive study and comparison. *Proceedings of 2020 5th International Conference on Cloud Computing and Artificial Intelligence: Technologies and Applications, CloudTech 2020*. https://doi.org/10.1109/CloudTech49835.2020.9365884

Tu, S., Waqas, M., Lin, Q., Rehman, S. U., Hanif, M., Xiao, C., … Chang, C. C. (2020). Tracking area list allocation scheme based on overlapping community algorithm. *Computer Networks*, *173*(February), 107182. https://doi.org/10.1016/j.comnet.2020.107182

Tymochko, A., Dudenko, S., Bodiak, O., & Perepelitsa, A. (2018). Mandatory resource access control based on a reachability matrix in storage area networks. In *Proceedings of 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies, DESSERT 2018* (pp. 539–543). https://doi.org/10.1109/DESSERT.2018.8409191

Ur, A., Khan, R., Othman, M., Madani, S., & Khan, S. U. (2014). A Survey of Mobile Cloud Computing Application Models. *IEEE Communications Surveys & Tutorials*, *16*(1), 393–413. https://doi.org/10.1109/SURV.2013.062613.00160

Veloudis, S., Paraskakis, I., Petsos, C., Verginadis, Y., Patiniotakis, I., Gouvas, P., & Mentzas, G. (2019). Achieving security-by-design through ontology-driven attribute-based access control in cloud environments. *Future Generation Computer Systems*, *93*, 373–391. https://doi.org/10.1016/j.future.2018.08.042

Venkata Giri, J., & Murty, A. S. R. (2020). An Evaluation of Security Key in Mobile Cloud. *Proceedings - 5th IEEE International Conference on Recent Trends in Electronics, Information and Communication Technology, RTEICT 2020*, 265–268. https://doi.org/10.1109/RTEICT49044.2020.9315553

Verma, A. K., & Garg, A. (2017). IPFS AND SWARM : FUTURE OF DECENTRALIZED STORAGE SYSTEM. *International Journal of Engineering Research in Computer Science and Engineering*, *4*(11), 14–17.

Vermeulen, S. (2020). *SELinux System Administration 3rd Edition*.

Wang, B., Yu, S., Lou, W., & Hou, Y. T. (2014). Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud. *Proceedings - IEEE INFOCOM*, 2112–2120. https://doi.org/10.1109/INFOCOM.2014.6848153

Wang, H., Ning, J., Huang, X., Wei, G., Poh, G. Sen, & Liu, X. (2019). Secure Fine-grained Encrypted Keyword Search for e-Healthcare Cloud. *IEEE Transactions on Dependable and Secure Computing*, (1), 1.

Wang, K., Wang, X., Liu, X., & Jolfaei, A. (2020). Task offloading strategy based on reinforcement learning computing in edge computing architecture of internet of vehicles. *IEEE Access*, *8*, 173779–173789. https://doi.org/10.1109/ACCESS.2020.3023939

Wang, P., Yue, Y., Sun, W., & Liu, J. (2019). An Attribute-Based Distributed Access Control for Blockchain-enabled IoT. *2019 International Conference on Wireless Annd Mobile Computing, Networking and Communication*, 1–6.

Wang, R., Azab, A. M., Enck, W., Li, N., & Chen, X. (2017). SPOKE : Scalable Knowledge Collection and Attack Surface Analysis of Access Control Policy for Security Enhanced Android. In *ACM on Asia Conference on Computer and Communications Security* (pp. 6126–624). ACM.

Wang, Shangping, Zhang, Y., & Zhang, Y. (2018). A Blockchain-Based Framework for Data Sharing with Fine-grained Access Control in Decentralized Storage Systems. *IEEE Access*, *6*, 38437–38450. https://doi.org/10.1109/ACCESS.2018.2851611

Wang, Shuo, Zhang, X., Zhang, Y., Wang, L., Yang, J., & Wang, W. (2017). A Survey on Mobile Edge Networks : Convergence of Computing , Caching and Communications. *IEEE Access*, *3536*, 1–21. https://doi.org/10.1109/ACCESS.2017.2685434

Wang, Y., Ma, Y., Xiang, K., & Liu, Z. (2018). A Role-Based Access Control System Using Attribute-Based Encryption. *International Conference on Big Data and Artificial Intelligence*, 128–133.

Waters, B. (2011). Ciphertext-Policy Attribute-Based Encryption : An Expressive , Efficient , and Provably Secure Realization. In *International Workshop on Public Key Cryptography* (Vol. 02, pp. 53–70). Springer.

Wilkinson, S. (2014). Storj A Peer-to-Peer Cloud Storage Network (pp. 1–18).

Wu, A., Zhang, Y., Zheng, X., Guo, R., Zhao, Q., & Zheng, D. (2019). Efficient and privacy-preserving traceable attribute-based encryption in blockchain. *Annals of Telecommunications*.

Wu, F., Luo, F., Chen, K., Lin, W., & Lu, Z. (2019). A Light-weight Kernel-level Mandatory Access Control Framework for Android. In *2019 IEEE International Conference on Power, Intelligent Computing and Systems, ICPICS 2019* (pp. 353–358). IEEE. https://doi.org/10.1109/ICPICS47731.2019.8942499

Wu, Z., Zhang, Y., & Xu, E. (2020). Multi-authority revocable access control method based on CP-ABE in NDN. *Future Internet*, *12*(1). https://doi.org/10.3390/fi12010015

Xie, M., Ruan, Y., Hong, H., & Shao, J. (2021). A CP-ABE scheme based on multi-authority in hybrid clouds for mobile devices. *Future Generation Computer Systems*, *121*, 114–122. https://doi.org/10.1016/j.future.2021.03.021

Xie, Y., Wen, H., Wu, B., Jiang, Y., & Meng, J. (2019). A modified hierarchical attribute-based encryption access control method for mobile cloud computing. *IEEE Transactions on Cloud Computing*, *7*(2), 383–391. https://doi.org/10.1109/TCC.2015.2513388

Xu, J., Xue, K., Li, S., Tian, H., Hong, J., Hong, P., & Yu, N. (2019). Healthchain: A Blockchain-Based Privacy Preserving Scheme for Large-Scale Health Data. *IEEE Internet of Things Journal*, *6*(5), 8770–8781. https://doi.org/10.1109/JIOT.2019.2923525

Xu, S., Ning, J., Li, Y., Zhang, Y., Xu, G., Huang, X., & Deng, R. (2020). Match in My Way: Fine-Grained Bilateral Access Control for Secure Cloud-Fog Computing. *IEEE Transactions on Dependable and Secure Computing*, *5971*(c), 1–13. https://doi.org/10.1109/TDSC.2020.3001557

Xu, S., Yang, G., Mu, Y., & Deng, R. H. (2018). Secure Fine-Grained Access Control and Data Sharing for Dynamic Groups in the Cloud. *IEEE Transactions on Information Forensics and Security*, *13*(8), 2101–2113. https://doi.org/10.1109/TIFS.2018.2810065

Xu, Y., Zeng, Q., Wang, G., Zhang, C., Ren, J., & Zhang, Y. (2020). An efficient privacy-enhanced attribute-based access control mechanism. *Concurrency Computation* , *32*(5), 1–10. https://doi.org/10.1002/cpe.5556

Xue, K., Hong, J., Xue, Y., Wei, D. S. L., Yu, N., & Hong, P. (2017). CABE: A New Comparable Attribute-Based Encryption Construction with 0-Encoding and 1-Encoding. *IEEE Transactions on Computers*, *66*(9), 1491–1503. https://doi.org/10.1109/TC.2017.2693265

Xue, K., Xue, Y., Hong, J., Li, W., Yue, H., Wei, D. S. L., & Hong, P. (2016). RAAC : Robust and Auditable Access Control with Multiple Attribute Authorities for Public Cloud Storage. *IEEE Transactions on Information Forensics and Security*, *6013*, 1–15. https://doi.org/10.1109/TIFS.2016.2647222

Yan, X., Yuan, X., Zhang, Q., & Tang, Y. (2020). Traceable and Weighted Attribute-Based Encryption Scheme in the Cloud Environment. *IEEE Access*, *8*, 38285–38295. https://doi.org/10.1109/ACCESS.2020.2975813

Yang, C., Tan, L., Shi, N., Xu, B., Cao, Y., & Yu, K. (2020). AuthPrivacyChain: A Blockchain-Based Access Control Framework with Privacy Protection in Cloud. *IEEE Access*, *8*, 70604–70615. https://doi.org/10.1109/ACCESS.2020.2985762

Yang, K., Han, Q., Li, H., Zheng, K., Member, S., & Su, Z. (2016). An Efficient and Fine-Grained Big Data Access Control Scheme With Privacy-Preserving Policy. *IEEE Internet of Things Journal*, *4*(April), 563–571. https://doi.org/10.1109/JIOT.2016.2571718

Yang, K., Jia, X., Ren, K., & Zhang, B. (2013). DAC-MACS : Effective Data Access Control for Multi-Authority Cloud Storage Systems. In *2013 Proceedings IEEE INFOCOM* (pp. 2895–2903).

Yang, T., Shen, P., Tian, X., & Chen, C. (2017). A Fine-grained Access Control Scheme for Big Data Based on Classification Attributes. In *IEEE 37th International Conference on Distributed Computing Systems Workshops* (pp. 238–245). IEEE. https://doi.org/10.1109/ICDCSW.2017.17

Yu, R., Qin, S., Bennis, M., Chen, X., Feng, G., Han, Z., & Xue, G. (2016). Enhancing Software-Defined RAN with Collaborative Caching and Scalable Video Coding. In *IEEE International Conference on Communications (ICC)* (Vol. 1457262, pp. 1–6). Kuala Lumpur: IEEE.

Yuan, C., Xu, M., Si, X., & Li, B. (2017). Blockchain with Accountable CP-ABE : How to Effectively Protect the Electronic Documents. In *23rd International Conference on Parallel and Distributed Systems* (pp. 800–803). IEEE. https://doi.org/10.1109/ICPADS.2017.00111

Zahed, N., Aminian, M., & Javadi, B. (2020). Journal of Network and Computer Applications Blockchain-based decentralized storage networks : A survey. *Journal of Network and Computer Applications*, *162*(September 2019), 102656. https://doi.org/10.1016/j.jnca.2020.102656

Zhang, J., Ma, J., Ma, Z., Lu, N., Yang, Y., Li, T., & Wei, D. (2019). Efficient hierarchical data access control for resource-limited users in cloud-based e-health. *Proceedings - 2019 International Conference on Networking and Network Applications, NaNA 2019*, 319–324. https://doi.org/10.1109/NaNA.2019.00062

Zhang, M., Luo, H., & Zhang, H. (2015). A Survey of Caching Mechanisms in Information-Centric Networking. *IEEE COMMUNICATION SURVEYS & TUTORIALS*, *17*(3), 1473–1499.

Zhang, P., Chen, Z., Liu, J. K., Liang, K., & Liu, H. (2016). An efficient access control scheme with outsourcing capability and attribute update for fog computing. *Future Generation Computer Systems*, *78*, 753–762. https://doi.org/10.1016/j.future.2016.12.015

Zhang, R., Ma, H., & Lu, Y. (2017). Fine-Grained Access Control System based on Fully Outsourced Attribute-Based Encryption. *The Journal of Systems & Software*, *125*(March), 344–353. https://doi.org/10.1016/j.jss.2016.12.018

Zhang, W., Wen, Y., Guan, K., Kilper, D., Member, S., Luo, H., & Wu, D. O. (2013). Energy-Optimal Mobile Cloud Computing under Stochastic Wireless Channel. *IEEE Transactions on Wireless Communications*, *12*(9), 4569–4581.

Zhang, X., Wu, F., Yao, W., Wang, Z., & Wang, W. (2019). Multi-authority attribute-based encryption scheme with constant-size ciphertexts and user revocation. *Concurrency Computation* , *31*(21), 1–9. https://doi.org/10.1002/cpe.4678

Zhang, Y., Deng, R. H., Xu, S., Sun, J., Li, Q., & Zheng, D. (2020). Attribute-based Encryption for Cloud Computing Access Control: A Survey. *ACM Computing Surveys*, *53*(4). https://doi.org/10.1145/3398036

Zhang, Y., Zheng, D., Chen, X., Li, J., & Li, H. (2014). Computationally efficient ciphertext-policy attribute-based encryption with constant-size ciphertexts. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (Vol. 8782, pp. 259–273). https://doi.org/10.1007/978-3-319-12475-9_18

Zhang, Y., Zheng, D., & Deng, R. H. (2018). Security and Privacy in Smart Health : E ffi cient Policy-Hiding Attribute-Based Access Control. *IEEE Internet of Things Journal*, *3*(1), 1–15. https://doi.org/10.1109/JIOT.2018.2825289

Zheng, H., Shao, J., & Wei, G. (2020). Attribute-based encryption with outsourced decryption in blockchain. *Peer-to-Peer Networking and Applications*, *13*(5), 1643–1655. https://doi.org/10.1007/s12083-020-00918-1

Zheng, Z., Xie, S., Dai, H.-N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities : a survey. *Int. J. Web and Grid Services*, *14*(4), 352–375.

Zhong, H., Zhu, W., Xu, Y., & Cui, J. (2018). Multi-authority attribute-based encryption access control scheme with policy hidden for cloud storage. *Soft Computing*, *22*(1), 243–251. https://doi.org/10.1007/s00500-016-2330-8

Zhou, K., & Ren, J. (2016). Secure Fine-Grained Access Control of Mobile User Data through Untrusted Cloud. In *25th International Conference on Computer Communication and Networks (ICCCN)* (pp. 1–9). IEEE.

Zhou, Zhenyu, Wang, B., Gu, B., Ai, B., Mumtaz, S., Rodriguez, J., & Guizani, M. (2020). Time-Dependent Pricing for Bandwidth Slicing under Information Asymmetry and Price Discrimination. *IEEE Transactions on Communications*, *68*(11), 6975–6989. https://doi.org/10.1109/TCOMM.2020.3001050

Zhou, Zhibin, Huang, I. D., & Wang, Z. (2013). Efficient Privacy-Preserving Ciphertext-Policy Attribute Based Encryption and Broadcast Encryption. *IEEE Transactions on Computers*.

Zhu, L., He, P., Hei, X., Yao, Y., Wang, Y., Ji, W., … Pan, L. (2020). Combined access control model embedding configurable policy for fine-grained data security. *Microprocessors and Microsystems*. https://doi.org/10.1016/j.micpro.2020.103060

Zickau, S., Thatmann, D., Butyrtschik, A., Denisow, I., & Axel, K. (2016). Applied Attribute-based Encryption Schemes. In *19th International ICIN Conference - Innovations in Clouds, Internet and Networks* (pp. 1–3). Paris.

Zyskind, G., Nathan, O., & Pentland, A. S. (2015). Decentralizing privacy: Using blockchain to protect personal data. In *2015 IEEE Security and Privacy Workshops* (pp. 180–184). IEEE. https://doi.org/10.1109/SPW.2015.27

BIODATA OF STUDENT

Fara Jamal received her Bachelor of Science (B.Sc.), in the field of Information Technology(Networking), from Universiti Utara Malaysia in 2001. She completed her Master of Science (M.Sc.), in the field of Information Technology majoring in Security, from Universiti Utara Malaysia in 2005. In 2004, she joined one of the Ministry in Malaysian Public Sector in Putrajaya, where she is a System Analyst and in charge of the Data Centre, Network and Security for more than 13 years.

She is currently joined the Faculty of Computer Science and Information Technology, Universiti Putra Malaysia to continue her study of Doctor of Philosophy (Ph.D.) in the field of Security in Computing. Her research interests lie in the area of Access Control in Mobile Cloud Computing, Encryption and BYOD security. She also serves as a reviewer for IEEE Access and Computers & Security Journal.

LIST OF PUBLICATIONS

Jamal, F., Abdullah, M. T., Hanapi, Z. M., & Abdullah, A. (2019). Reliable Access Control for Mobile Cloud Computing (MCC) With Cache-Aware Scheduling. *IEEE Access*, *7*, 165155–165165.

Jamal, F., Abdullah, M. T., Abdullah, A., & Hanapi, Z. M. (2018). BYOD Authentication Process (BAP) Using Blockchain Technology. *Journal of Adv Research in Dynamical & Control Systems*, *10*(11), 166–172.

Jamal, F., Abdullah, M. T., Abdullah, A., & Hanapi, Z. M. (2018). Enhanced Bring your Own Device (BYOD) Environment Security based on Blockchain Technology. *International Journal of Engineering & Technology*, *7*, 74–79.

Jamal, F., Abdullah, M. T., Abdullah, A., & Hanapi, Z. M. (2020). A Systematic Review Of Bring Your Own Device (BYOD) Authentication Technique A Systematic Review Of Bring Your Own Device (BYOD) Authentication Technique. *Journal of Physics*, *1529*.

Jamal, F., Abdullah, M. T., Abdullah, A., & Hanapi, Z. M. (2020). Secure Multi-authority Attribute- Based Encryption With Cache-aware Scheduling For Mobile Cloud Access Control. *International Journal of Advanced Research in Engineering and Technology (IJARET).*

UNIVERSITI PUTRA MALAYSIA

STATUS CONFIRMATION FOR THESIS / PROJECT REPORT AND COPYRIGHT

ACADEMIC SESSION: Second Semester 2020/2021

TITLE OF THESIS / PROJECT REPORT:

SECURE MULTI-AUTHORITY ATTRIBUTE-BASED ENCRYPTION ACCESS CONTROL WITH CACHE-AWARE SCHEDULING IN MOBILE CLOUD COMPUTING

NAME OF STUDENT: FARA BINTI JAMAL

I acknowledge that the copyright and other intellectual property in the thesis/project report belonged to Universiti Putra Malaysia and I agree to allow this thesis/project report to be placed at the library under the following terms:

1. This thesis/project report is the property of Universiti Putra Malaysia.
2. The library of Universiti Putra Malaysia has the right to make copies for educational purposes only.
3. The library of Universiti Putra Malaysia is allowed to make copies of this thesis for academic exchange.

I declare that this thesis is classified as:

*Please tick (√)

☐	**CONFIDENTIAL**	(Contain confidential information under Official Secret Act 1972).
☐	**RESTRICTED**	(Contains restricted information as specified by the organization/institution where research was done).
☑	**OPEN ACCESS**	I agree that my thesis/project report to be published as hard copy or online open access.

This thesis is submitted for:

☐	**PATENT**	Embargo from _____ until _____ (date) (date)

Approved by:

_____	_____
(Signature of Student)	(Signature of Chairman of Supervisory Committee)
New IC No/ Passport No.:	Name:
Date:	Date:

[Note: If the thesis is CONFIDENTIAL or RESTRICTED, please attach with the letter from the organization/institution with period and reasons for confidentially or restricted.]