

**UNIVERSITI TEKNOLOGY MARA**

**CRYPTO E-PASSPORT USING BLOCKCHAIN BASED SYSTEM**

**SHARIFAH HASYIMAH BINTI SYED MOHD KHALID**

**Bachelor of Computer Science (Hons.) Data Communication and Networking (CS245)**

**28 July 2020**

## **ACKNOWLEDGEMENT**

Alhamdulillah , with Allah S.W.T blessing, I managed to finish this research within the duration of the time given. Special thanks and appreciation to my supervisor , En Mohamad Yusuf Darus with his endless advice and support that was given to me to complete this project.

Must not forget to thank my beloved mother that always offer a sincere advice and support that give me strength to complete this research.

My utmost gratitude towards all my friend that involved in helping to perfecting this research and for the endless emotional support during completing this research.

## ABSTRACT

Passport is one of the most important things for the country. It was issued for their citizen that verifies the identity and nationality of the holder on international level. With this document, it will grant its owner a safe passage and protection in a foreign land. Without this document, people will be banned from entering or exiting the country. However, there is a rising problem of fake passport. People who travel with fake passport are usually trying to hide their identity such as a refugee or a terrorist. It is dangerous for criminals that have a bad intention to enter the country. It can cause chaos to the nation. The use of fake passport is not unfamiliar things. There are many cases where people who conduct an illegal operation in some part of the country are using a fake passport such as the missing MH370 planes involving two Iranians that exposed a two Iranian that bought a fake passport. Many technologies have been developed to combat counterfeit passport syndicates such as e-Passport or electronic passport that was developed as two factor verification for immigration to fully verify the originality of the passport. But is it secure? In 2007 an RFID expert Lukas Grunwald demonstrated how he crashed the passport reader at the immigration by infecting a forged chip with a malicious code and crashing the passport reader. This incident suggests that the reader is vulnerable to code injection that can reprogram the reader to approve a forged passport as a genuine one. A rising blockchain smart contract that appears secure and reliably fast technology by Ethereum. A smart contract allows the program or data being stored in the blockchain block that is decentralized and heavily encrypted. So, an additional measure was suggested by this project to fully take advantage of secure blockchain framework as a third factor to verify the genuineness of the passport.

# Table of Contents

<b>FRONT PAGE</b> .....	<b>I</b>
<b>SUPERVISOR APPROVAL</b> .....	<b>II</b>
<b>STUDENT DECLARATION</b> .....	<b>III</b>
<b>ACKNOWLEDGEMENT</b> .....	<b>IV</b>
<b>ABSTRACT</b> .....	<b>V</b>
<b>TABLE OF CONTENTS</b> .....	<b>VI</b>
<b>LIST OF FIGURES</b> .....	<b>VIII</b>
<b>LIST OF TABLES</b> .....	<b>IX</b>
<b>CHAPTER 1: INTRODUCTION</b> .....	<b>1</b>
1.1 Background of Study.....	1
1.2 Problem Statement.....	2
1.3 Research Question.....	2
1.4 Research Aim .....	2
1.4.2 Research Objectives.....	2
1.5 Research Scope and Limitations.....	3
1.6 Significance of Study .....	3
<b>CHAPTER TWO: LITERATURE REVIEW</b> .....	<b>4</b>
2.1 Introduction .....	4
2.2 The CIA Principle .....	4
2.3 Introduction of E-Passport System .....	6
2.4 Type of Attack.....	6
2.5 Technology Use.....	5
2.6 Comparison of Related Works.....	8
<b>CHAPTER THREE: METHODOLOGY</b> .....	<b>24</b>
3.1 Overview of Research Methodology .....	24
3.2 Project Flow Diagram .....	24
3.3 Framework of Research Methodology .....	25
3.4 Feasibility Studies Phase.....	26
3.5 Design Phase.....	27
3.6 Development Phase.....	39
3.7 Performance Evaluation Phase.....	48
3.8 Documentation Phase .....	48
3.9 Summary.....	48

# CHAPTER 1

## INTRODUCTION

### 1.1 Background of Study

Electronic passport is one of a method use as a government official document to verify and certify identification of local and foreign people in and out of a country. The current existing system have flaws that can be exploit by hackers. These flaws are dangerous because it may lead to multiple data privacy threats. The threat can be i.e.; e fake passport, smart electronic chip exploit by hacker and allow hacker to retrieve and manipulate passport information. In 2015, researcher from Concordia University said one of the vulnerabilities is Radio Frequency Identification (RFID) Enable passports has several vulnerability problems that can compromise the security of the passport. Each passport smart chip data is secure by unique encryption code. However due to fast growth of digital technology even the secure encryption code can be hacked by expert. Moreover, the current database of passport information uses a centralized database, with operated by authorized human interface that may lead to internal security breach. Due to the possibility of internal security breach the data integrity can be question. Furthermore, the centralized server has a physically form and can be targeted by the hacker.

Different from crypto e-blockchain based system technology, Crypto are form of digital. Crypto don't require a central authority and protected by complex hash algorithm that are possible can be crack by the hacker. Blockchain provide a way to record and transfer data that is transparent, safe, auditable and resistant to outages. Blockchain has the ability to make the organizations that use it transparent, decentralized efficient and secure. It's a technology that hold a lot of promise for the future and it is already disrupting many industries.

In 2014, Malaysia Airlines MH370 has an issue about two men travelling on stolen passports. In a way these two individuals with stolen passports on a plane was a breach of security. This show current verification system has flaw because of the verification are not synchronize in real time with Interpol stolen passport databased.

Smart Contract is the key technology innovation and second-generation blockchains has been developed. Smart contract is computer code that is stored inside of a blockchain which encode contractual agreement smart contract are self-executing with the term of the agreement or operation directly written into line of code stored and executed on the blockchain computer.

QR code implementation is used for as an additional factor of authentication to verify the authenticity of the passport. With added authentication factor, this will strengthen the passport verification system at the immigration side. The QR code contain a verification link to the blockchain server to further check the authenticity of the passport. QR code was used since it is not device oriented and able to be used by major device for verification. This will not in cure additional charge for the additional device.