Zero Knowledge Protocol
Network Authentication and Monitoring

BY

ANG YONG SENG

A REPORT

SUBMITTED TO

Universiti Tunku Abdul Rahman

in partial fulfillment of the requirements

for the degree of

BACHELOR OF INFORMATION TECHNOLOGY (HONOURS) COMMUNICATIONS AND NETWORKING

Faculty of Information and Communication Technology

(Kampar Campus)

JAN 2024

UNIVERSITI TUNKU ABDUL RAHMAN

REPORT STATUS DECLARATION FORM

Title: Zero Knowledge Protocol Network Authentication and Monitoring

Academic Session: January 2024

I ___ANG YONG SENG_______________________________________

(CAPITAL LETTER)

declare that I allow this Final Year Project Report to be kept in
Universiti Tunku Abdul Rahman Library subject to the regulations as follows:

1. The dissertation is a property of the Library.
2. The Library is allowed to make copies of this dissertation for academic purposes.

Verified by,

GML

(Author's signature)

(Supervisor's signature)

Address:
_112, Jalan Taman Bintang 1, Fasa 1, _
_34900, Pantai Remis, _____________
_Perak Darul Ridzuan. _____________

_Ts. Dr. Gan Ming Lee ____
Supervisor's name

Date: __18/04/2024________________

Date: __26/4/2024________

Universiti Tunku Abdul Rahman			
Form Title : **Sample of Submission Sheet for FYP/Dissertation/Thesis**			
Form Number: **FM-IAD-004**	Rev No.: **0**	Effective Date: **21 JUNE 2011**	Page No.: **1 of 1**

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY

UNIVERSITI TUNKU ABDUL RAHMAN

Date: _26/04/2024_________________

SUBMISSION OF FINAL YEAR PROJECT /DISSERTATION/THESIS

It is hereby certified that ______***Ang Yong Seng***___________ (ID No: __***20ACB02293***___) has completed this final year project entitled "__Zero Knowledge Protocol Network Authentication and Monitoring _" under the supervision of __Ts. Dr. Gan Ming Lee _______________ (Supervisor) from the ____Department of _Computer and Communication Technology____, Faculty of ____Information and Communication Technology_______.

I understand that University will upload softcopy of my final year project in pdf format into UTAR Institutional Repository, which may be made accessible to UTAR community and public.

Yours truly,

____

(*Ang Yong Seng*)

DECLARATION OF ORIGINALITY

I declare that this report entitled "**ZERO KNOWLEDGE PROTOCOL NETWORK AUTHENTICATION AND MONITORING**" is my own work except as cited in the references. The report has not been accepted for any degree and is not being submitted concurrently in candidature for any degree or other award.

Signature : ______________________________

Name : _Ang Yong Seng____________

Date : __18/04/2024_______________

ACKNOWLEDGEMENTS

Thanks a lot, to my supervisor, Ts. Dr. Gan Ming Lee guided me throughout the ZKP authentication and monitoring project. He encouraged me to think critically and independently throughout the project. I am appreciative of his patience in providing me guidance when I was having misunderstood on some concepts throughout the implementation. Since it is my first long-term project, it is a valuable exposure and experience for me.

My family members' support is encouraging and allows me to keep moving forward when facing any challenge in the course. I am immensely appreciative of their unconditional patience and care; it makes me learn from them and persist on the project's objectives.

ABSTRACT

The network has become more prominent and more accessible to every layer of society. As the number of users has increased, more data flows between the network, leading to a spike in security issues. The advent of network authentication and network monitoring has helped address these concerns. However, some existing network authentication schemes are applying weak password and not adhering to the standard password policy, causing the overall security level has been decreased. In this project, the network authentication will be integrated with the Zero Knowledge Protocol (ZKP) assisted by RSA authentication scheme. Hence, the overall security level of the network authentication can be improved as compared to username/password authentication. Network monitoring plays a significant role in analyzing resource usage of hosts inside the local network. It allows the network administrator to monitor and detect potential anomalies occurred in the local network, so that the network administrator could take further action according to organization policy. In this project, Zabbix will play a pivotal role for displaying the dashboard to the network administrator.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

5G	Fifth Generation
AS	Authentication Server
CHAP	Challenge Handshake Authentication Protocol
ECC	Elliptic Curve Cryptography
HR	Human Resources
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ID	Identification
IoV	Internet of Vehicles
MITM	Man-In-The-Middle
NFV	Network Functions Virtualization
OTP	One-Time-Passwords
PAP	Password Authentication Protocol
PEM	Private Enhanced Mail
PKI	Public Key Infrastructure
RSA	Rivest, Shamir, and Adleman
RFID	Radio-Frequency Identification
SDLC	Software Development Life Cycle
SDN	Software-Defined Networking
SP	Service Provider
SPKI	Simple Public Key Infrastructure
SSL	Secure Socket Layer
TA	Trusted Authority
VU	Vehicular User
XOR	Exclusively-OR
ZAMA	ZKP-Based Anonymous Mutual Authentication
ZKP	Zero Knowledge Proof

Chapter 1

Introduction

In this chapter, we discuss the problem statement and the motivation behind the research project. To dive deeper into the project related information, the chapter will include the research objectives, project scope and direction. Meanwhile, the contribution of research to the relevant field will be proposed. Next, the thesis outline will be organized and stated at the end of chapter.

1.1 Problem Statement and Motivation

Weakness in Password Security

Implementing traditional username and password authentication methods exposes users to a broad range of security breaches. Humans tend to prefer simple passwords that are easily remembered or use the same password for multiple platforms, making them susceptible to security risks such as brute force attacks. Additionally, password-based authentication methods can be vulnerable to cyber attacks due to their easy-to-guess password combinations. Overall, username and password authentication are not reliable as user identity and access mechanisms in today's landscape. In year 2020, the percentages of data breaches associated with hacking via brute force attacks and exploitation of weak passwords is over 80% [1]. If users choose weak or easily guessable passwords, attackers can exploit this vulnerability through brute-force attacks, dictionary attacks, or password guessing due to the limited password character combinations. Consequently, malicious hackers can easily exploit weaknesses in password security.

Single Point of Failure in Database Storage

Conventional authentication methods, such as password-based or biometric authentication, require users to provide specific credentials for authentication whenever they set up user authentication. These credentials are typically stored in a centralized database, directory service, or identity management system. This storage method allows the authentication server to compare the user's credentials with those stored in the database, enabling authorized users to access the network. However, large-scale data breaches can occur if malicious attackers access the stored credentials. According to Resecurity [2], two of the largest data center operators in Asia, Shanghai-based GDS Holdings and Singapore-based ST Telemedia Global, were accessed by malicious hackers. Consequently, the hackers were able to obtain the credentials used for customer support login, leading to identity theft. Additionally, the company's network could also be accessed, potentially causing the leakage of intellectual property. Undoubtedly, significant data breaches negatively affect investor confidence in the company, leading to a loss of trust among customers and investors. In short, storing passwords or other credentials in single database poses a significant security risk as the database could become a single point of failure.

1.2 Objectives

The project aims to propose an authentication protocol for network access using Zero Knowledge Proof (ZKP) technology. In this project, the RSA authentication scheme will be utilized for the purpose of ZKP implementation. With the ZKP technology assisted by RSA authentication scheme, users are not required to reveal private key to server during authentication, so their authentication credentials like private key will not be exposed to eavesdropping attack. In this project, the public key will be exposed to the centralized databases, mainly for verification purpose. By implementing the ZKP with RSA authentication scheme, it will allow the whole authentication process to be simplified because the RSA asymmetric key pair will be generated by server and distributed to the respective user. Thus, ZKP authentication provide convenience to users since they are not required to remember any username and password.

Furthermore, the project aims to avoid the storage of a private key into a single database, while ensuring the private key recoverability in case the user has accidentally deleted their private key. In this project, the private key will be stored in the server database, so that the user is able to retrieve the private key again from the system. To further assure the private key protection, the private key will be separated into several parts, and stored in different databases, by referencing to the concept of Shamir's secret sharing. The private key could be recovered when there is sufficient piece of information, without having a single database holding all the data [3]. Hence, it can increase the difficulty level in accessing the user private key, while ensuring the private key recoverability.

1.3 Project Scope and Direction

The proposed project involved two parts such as network authentication and network monitoring. However, the majority part will emphasise on the network authentication, while network monitoring will not have much emphasises throughout the project. The project scope includes implementing a ZKP authentication scheme for network access. Instead of using complex mathematical formulas, public key cryptography, a cryptographic algorithm, will be applied to the project for authentication purposes. The signing and verification processes using public and private keys can authenticate the users effectively without compromising credential information. A captive portal is constructed and hosted locally using Visual Studio Code to conduct testing for the network authentication process. The project scope is only limited to HTTP traffic. Besides, to maintain the state for a user to be authenticated, the source IP address of incoming requests will be checked and performed the comparison with session table in database.

However, ZKP will not be included in the implementation of network monitoring; instead, the part of network monitoring will be focused on displaying the proxy server status such as resource usage via the Zabbix dashboard. Other than that, machine learning techniques for detecting security threats in network logging are outside the scope of the project.

1.4 Contributions

The main contribution of this project is implementing network authentication using ZKP technology with RSA authentication scheme. RSA is considered as a secure authentication scheme for common computational power in current era. RSA authentication enables more possible combinations, heightening the difficulty level to crack its encryption and requiring more computational efforts in brute-force attack. In short, it enhances the overall security for network authentication purpose, as compared to username and password authentication.

Other than that, the private key recoverability is included as one of the key contributions via this project. In public key cryptography, private key of a user is acknowledged as a sensitive secret which is prohibited to share with others. However, the project will separate the private key of each user and further distribute into different databases. Hence, the malicious hacker is not able to retrieve a complete piece of private key even they have accessed into one of the databases with an unauthorized mean. In summary, the contribution mentioned enable the private key recoverability of a user, while avoiding a single point of failure from databases.

1.5 Report Organization

The organization of the report are mainly distributed into seven chapters. The report begins with Chapter 1 Introduction, Chapter 2 Literature Review, Chapter 3 System Methodology/Approach, Chapter 4 System Design, Chapter 5 System Implementation, Chapter 6 System Evaluation and Discussion, and Chapter 7 Conclusion and Recommendation. The following chapters will further delve into the details of the project in different perspectives. At the beginning, Chapter 1 outlines the introduction and purpose regarding the proposed project. Next, Chapter 2 discusses the existing or past research which have been generated by other researchers. Furthermore, the approach adopted to develop the proposed system will be explained in detail via Chapter 3. After that, Chapter 4's system flow will be emphasised by using flowcharts, which are focused on user registration and authentication for network authentication, as well as network monitoring. Other than that, Chapter 5 covers the implementation of proposed system as well as discusses the challenges faced. By diving in further, the proposed system will be evaluated more towards the aspect of security in Chapter 6, accessing the system performance. Lastly, Chapter 7 will summarise again the overall significance in the research and mention recommendations for future work or action.

Chapter 2
Literature Review

2.1 ZAMA: A ZKP-Based Anonymous Mutual Authentication Scheme for the IoV

The authors [4] have identified a significant privacy concern regarding the vehicle's authentication, which is identity leakage. Due to the complex computation of the ZKP protocol, it is impractical to implement authentication methods in the Internet of Vehicles (IoV) system.

In the study [4], a novel ZKP-based anonymous authentication approach has been proposed for IoV. The authors have made several contributions through their system, such as applying ZKP and elliptic curve cryptography (ECC) to design an anonymous mutual authentication protocol for IoV. They also adopted a precalculated mechanism to reduce the burden of complex calculations, making the protocol lightweight. Furthermore, they built a fast reconnection protocol in the security context from the recent vehicle access. Finally, they deployed a ZKP-based anonymous mutual authentication scheme suitable for implementation in the IoV environment.

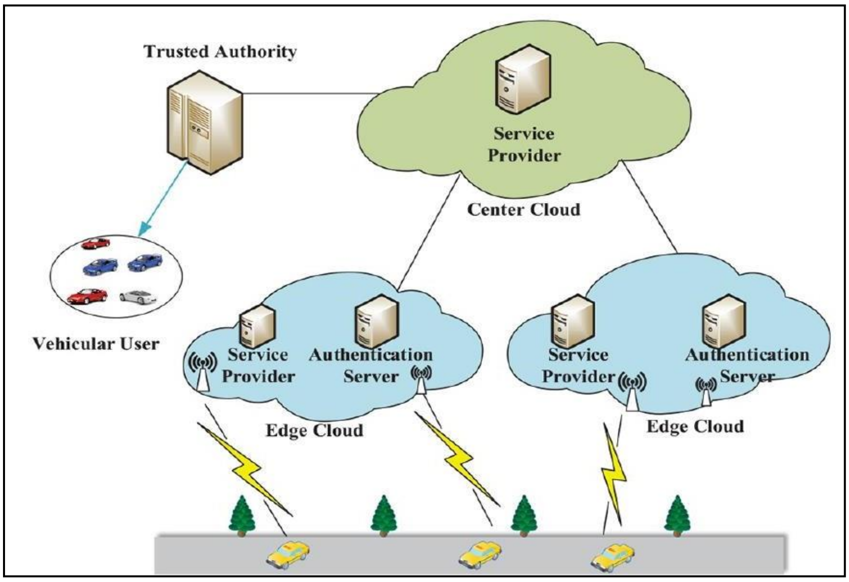


Figure 1.1: The IoV System’s Model

The model of the IoV system includes components like vehicular user (VU), trusted authority (TA), service provider (SP), and authentication server (AS), as demonstrated in Figure 1.1. Ning Xi et al. [4] aimed to achieve security goals by designing a novel anonymous authentication to eliminate insider and outsider threats during IoV authentication. The security goals consist of five components: mutual authentication, anonymity, unlinkability, traceability, and forward security. VU and AS must authenticate each other to identify whether either is illegal or fake. Furthermore, attackers can only obtain VU's pseudonyms, not relevant information on VU's real identity. The system also inhibits attackers from linking the VU even if the AS is compromised and wireless channel control occurs. Meanwhile, traceability refers to the TA's ability to trace the VU and hold them accountable when a violation occurs in the execution of IoV's services. For forward security, attackers cannot obtain any useful information about the previous session, even if they hold all information about the current session.

Based on the results analysis [4], the user's strong anonymity and authenticity are achieved using ZKP-Based Anonymous Mutual Authentication (ZAMA). User traceability can be assured by tracking users' verification keys when a violation occurs. Users can quickly reconnect to the IoV based on the security context from the last access, reducing computation overhead.

Strengths and Weaknesses

ZAMA for IoV has strengths such as traceability, anonymity, and lower computational power. However, the comparison will be performed from the aspects below, such as security, feasible computational cost, as well as private key recoverability. The authentication scheme being applied in the ZAMA for IoV is the ECC cryptographic scheme. Both are feasible for current computing devices in term of the computational cost. Other than that, ZAMA for IoV does not propose any solution to recover the private key in case user accidentally delete it.

However, ZKP Network Authentication has provided the feature of private key recoverability in comparison with ZAMA for IoV. In the proposed project, the private key will be separated into different parts and store into three databases by applying the Shamir's secret sharing concept. Hence, an unauthorized access into a single private key database will not cause a single point of failure, because the private key reconstruction is also required three pieces of separated shares stored in different databases.

Table 1.1: Comparison table between ZKP Network Authentication, and ZAMA for IoV

	ZKP Network Authentication	**ZAMA for IoV**
Security	✔	✔
Feasible computational cost	✔	✔
Private key recoverability	✔	

2.2 An Efficient Improvement of RFID Authentication Protocol Using Hash Function ZKP

The security and privacy of radio-frequency identification (RFID) remains a significant issue due to its wireless communication application. However, the previous works of the paper are still exposed to the vulnerability of multiple security and privacy attacks, such as man-in-the-middle (MITM) attacks. Hence, the authors [5] proposed to enhance an existing RFID authentication protocol via a mutual authentication protocol. By using the Tuyles and Batina protocol, the security and privacy issues can be improved. Meanwhile, the Keccak hash function is also applied to maintain mutual authentication between RFID tags and the reader during communication while maintaining the integrity of the exchanged message.

The proposed protocol [5] is a challenge-response protocol containing two stages - setup and authentication. First, the generation of an elliptical curve, the base point of the elliptic curve, and private and public keys will be implemented during the setup stage. For the authentication phase, it consists of two verification processes. The verification starts with checking whether the reader is legitimate, depending on the encryption's capability to compute the hash value. After that, the hash values of the encryption message are calculated and verified, followed by the computation of proving the challenge.

According to the results, the proposed protocol can resist multiple cyberattacks, such as man-in-the-middle attacks, tracking attacks, and impersonation attacks. The confidentiality and integrity level of the RFID authentication system has been enhanced as an impact. On the other hand, the proposed protocol supports anonymity and mutual authentication, leading to enhanced privacy protection.

Strengths and Weaknesses

RFID authentication protocol using hash function ZKP has better security by implementing a mutual authentication protocol. The mutual authentication between RFID tags and the reader can be maintained using the Keccak hash function. Meanwhile, ZKP network authentication applies the RSA authentication scheme, which are widely adopted and generally secure.

However, RFID authentication protocol using hash function ZKP requires moderate computational cost. The authentication phase consists of two verification processes. It is separated into the verification of hash values of the encryption message, followed by the computation of challenge verification. For ZKP network authentication, the stage of authentication is separated into challenge generation, signature signing, and signature verification involving the RSA authentication scheme. In overall, the computational cost is considered feasible for the general computing devices.

In terms of comparision, ZKP network authentication has offered user a way to recover the private key in case they are accidentally delete it. It allows users to obtain again their private key for authentication via registration steps. To make sure the storage of private keys secure, it is separated into three databases which avoiding a single point of failure.

Table 2.1: Comparison table between ZKP Network Authentication, and RFID Authentication Protocol using Hash Function ZKP

	ZKP Network Authentication	**RFID Authentication Protocol Using Hash Function ZKP**
Better security	✔	✔
Feasible computational cost	✔	✔
Private key recoverability	✔	

2.3 Zero-Knowledge Proof Based Authentication Over Untrusted Networks

The problem acknowledged by the authors [6] is that hashed passwords with associated usernames are still susceptible to attacks like packet sniffing and eavesdropping when stored and sent over an untrusted network. Therefore, the paper [6] proposes an idea that uses ZKP with improvisation and a combination of the Challenge Handshake Authentication Protocol (CHAP) and Password Authentication Protocol (PAP). The proposed approach in the paper is a mixture of CHAP, PAP, and ZKP. Furthermore, the method includes the additional features of XOR functionality and public key encryption.

Based on the proposed idea, the password authentication mechanism will be separated into 3 stage phases. The first stage is registration, which requires devices to register with the trusted server. Moving on to the next stage, the verification phase, the device's legitimacy can be verified. If the device is legitimate, it will proceed to the last stage, the authentication stage. During the authentication stage, the usage of resources will be a factor used to authenticate the device.

A comparative analysis has been carried out for the time taken in different stages, including registration, verification, and authentication of various devices by applying traditional and proposed ZKP authentication methods. Besides, a valid transaction column is inserted with a count of ten to ensure authentication. Multiple types of attacks have been prevented. For instance, spoofing-based attacks are prevented because the probability of a sequence of random bits being followed is very low, at 1/210. Additionally, the randomized bits generated in authentication have hindered replay attacks. Password-based attacks like brute-force attacks can be prevented since the password is no longer sent over an untrusted network.

Strengths and Weaknesses

ZKP, with the combination of CHAP and PAP, provides robust security by mixing the implementation between CHAP, PAP and ZKP. The deposit is further improved with XOR functionality and public key encryption features. The proposed solution in the previous work uses only ten random bits in authentication. Even though it might compromise security strength, it reduces the computational cost. Other than that, the usage of resources will be a factor used to authenticate the device during the authentication stage. However, the computational cost is generally feasible for the computing devices nowaday. From different perspectives, ZKP with the combination of CHAP and PAP is less efficient because it takes longer for authentication phases than traditional ZKP authentication schemes. The ZKP with the combination of CHAP and PAP does involve the public key encryption but does not offer users a mean to recover the private key in case they have accidentally delete the key.

Table 3.1: Comparison table between ZKP Network Authentication, and ZKP with the Combination of CHAP and PAP

	ZKP Network Authentication	**ZKP with the Combination of CHAP and PAP**
Better security	✔	✔
Feasible computational cost	✔	✔
Private key recoverability	✔	

2.4 Access Control in 5G Communication Networks Using Simple PKI Certificates

A heterogeneous network is applied for 5G mobile communications. Multiple platforms, technologies and cell sizes are being deployed to fit specific data rates and latency requirements. Many devices will be connected to the network, and IP-based communication architecture is applied. Therefore, there is a high potential for 5G wireless networks to be the target of known and unknown security attacks.

In the project [7], a simple public key infrastructure (PKI) certificate-based access control scheme is proposed for investigating an access control design and authentication scheme for a 5G communication network. A virtualization architecture is implemented via software-defined networking (SDN), OpenFlow, and network function virtualization (NFV). It boosts the efficiency of network management and control functions. The project's scope is the establishment of authentication and handover schemes in a scalable manner. Besides, various types of novel certificates are defined and come with specific features and utilizations. At the same time, a secure device registration process can be secured using ZKP before the generation of authorization certificates.

The project's contribution includes establishing the hierarchical architecture of 5G communication networks. For instance, virtualization concepts and orchestration of network management functions are implemented by investigating SDN and NFV paradigms. Furthermore, a simple PKI architecture is developed for the authentication and access control in 5G networks. A mechanism of authentication and registration using ZKP is created to authenticate the authorized users. The communication channel between devices is constructed with a secure certificate generated. Furthermore, a simple PKI certificate-based handover scheme is designed to meet the latency requirements of the 5G standard. In addition, a security scheme is proposed using SPKI by defining new types of certificates with innovative structures and semantics [7].

A simulation model is developed using Matlab to evaluate the proposed registration and authentication. Based on the performance evaluation, the total registration and authentication overhead and the latency of the proposed scheme have been compared. As a result, global registration and authentication overhead is reduced significantly via the project. Furthermore, the performance of the handover process is enhanced, mainly using simple PKI certificates for authentication. Due to the distributed model applied in the handover scheme, the number of exchanged messages and the delay in initiating the attachment procedure are reduced. Moreover, the proposed methods exhibit higher scalability than existing authentication and handover schemes. The proposed system has achieved higher security and scalability levels, but the communication overhead and average latency are being compromised.

Strengths and Weaknesses

The proposed method in article is considered secure due to the ZKP-based registration and authentication, as well as simple PKI certificates. However, the security level should be higher especially being in 5G networks that support tremendous users, which is a wireless network. The registration, authentication and handover mechanisms using simple PKI architectures only require less resources because there is a decrease in registration and authentication overhead, followed by lower latency produced.

Table 4.1: Comparison table between ZKP Network Authentication,
and Access Control in 5G Communication Networks Using Simple PKI Certificates

	ZKP Network Authentication	**Access Control in 5G Communication Networks Using Simple PKI Certificates**
Efficiency	✔	✔
Better security	✔	
Private Key Recoverability	✔	

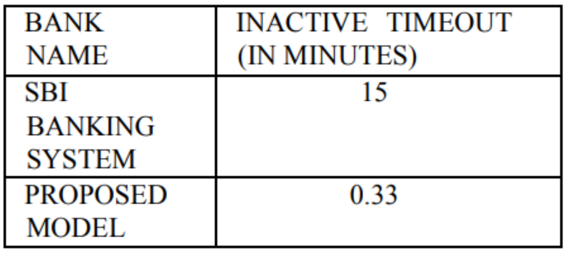
2.5 Application of Session Login and One Time Password in Fund Transfer System Using RSA Algorithm

The article delves into the advancements of banking security within authentication protocols [8] . It highlights a shift from traditional banking security algorithms to a two-key authentication system utilizing RSA encryption. The authors implement techniques like Time-based One-Time-Passwords (OTPs) and employ session logins to bolster security for fund transfers in the banking industry.

The proposed project in the article segregates modules into various segments targeting bank administrators and managers. These modules include the key generation module, database module, verification module, etc., accompanied by secure communication channels for key exchange. Additionally, the system integrates random password number generators with RSA authentication schemes and employs SSL security for transmitting RSA private keys.

The article discusses the implementation of OTP validity periods and session timeout features, significantly reducing compared to practices adopted by other banks. This reduction effectively diminishes the probability of being hacked since OTPs expire quickly and necessitate regeneration by the server for further usage. In summary, the banking security framework utilizing RSA authentication demonstrates a proactive approach to safeguarding sensitive financial activities such as fund transfers.

Table 5.1: Standard Comparison of inactivity logout time between existing system and article's proposed system



BANK NAME	INACTIVE TIMEOUT (IN MINUTES)
SBI BANKING SYSTEM	15
PROPOSED MODEL	0.33

Strengths and weaknesses

Due to nature of banking industry, the proposed system in the reviewed article utilises multiple security protection mechanisms to safeguard their data, including transaction data. Besides, the RSA authentication has also been integrated in random password number generators, providing a robust authentication scheme for the customer. Meanwhile, the session logins can become one of the proactive measures to maintain the state of authentication. According to the measures adopted above, it showcases a robust security mechanism in the banking industry. Nevertheless, due to multiple security mechanisms being implemented, it could lead to some level of difficulties in managing all those security measures.

Table 5.2: Comparison table between ZKP Network Authentication, and Application of Session Login and One Time Password in Fund Transfer System Using RSA Algorithm

	ZKP Network Authentication	**Application of Session Login and One Time Password in Fund Transfer System Using RSA Algorithm**
Better security	✔	✔
Efficiency	✔	
Private Key Recoverability	✔	

2.6 A User Convenient Secure Authentication Scheme for Accessing e-Governance Services

In government to citizen (G2C) e-Governance services, the users' credentials are required to be disclosured for registration purposes. Since G2C model involves multiple kind of services like e-health, the users are requested to go through the registration process once for every application service. It is totally inconvenient for user to memorize login credentials for each application service due to human nature which will forget the login credentials easily. It is undeniable that G2C model requires a user-friendly multi-server interaction with a suitable cryptographic approach to safeguard the data security.

Hence, the reviewed project [9] has proposed an RSA based multi-server authentication model which enables the user to access different services in a convenient way. Via the proposed mechanism in reviewed project [9], all the G2C e-Governance services will be accessible through a trustworthy agency or registration center. However, the user must register once with the registration center by providing the details of services that tend to access. The user made a request to the registration center to access particular e-service as proposed in reviewed article. After the verification by the trustworthy agency/registration center, user receives a token from the trustworthy agency or registration center for further verification process with the application server.

In authentication stage, the token assigned by the registration center will become a proof of mutual authentication between user and particular e-service. For every request to the e-Governance service, a request will be sent to the relevant application service together with the token assigned by registration center. A user will only provide once the login credentials to access all e-application of G2C e-Governance services within the session validity period. Based on the formal analysis done by author, the scheme can protect against active and passive cyber attacks like replay attack during the transmission over public channels. Furthermore, the scheme mentioned has shown better security and computation overhead compared to other schemes in the relevant field. Nevertheless, the scheme has introduced more bandwidth usage and latency while transmitting the encrypted information over the network.

Strengths and Weaknesses

To handle the G2C model, the reviewed article introduces a multi-server interaction with a suitable cryptographic approach to protect against the leak of users' data. In the reviewed article, the multi-server authentication model has adopted the RSA algorithm, showcasing a better security level. Meanwhile, the user is allowed to access all e-application of G2C e-Governance services after the user has registered once via registration center. From the opposite side, there are more bandwidth usage and latency to be used while transmitting the encrypted information over the network, indicating more communication costs required in the system.

Table 6.1: Comparison table between ZKP Network Authentication,

and A User Convenient Secure Authentication Scheme for Accessing e-Governance Services

	ZKP Network Authentication	**A User Convenient Secure Authentication Scheme for Accessing e-Governance Services**
Better security	✔	✔
Efficiency	✔	✔
Higher communication cost	✔	✔
Private Key Recoverability	✔	

2.7 Zero Knowledge Protocol with RSA Cryptography Algorithm for Authentication in Web Browser Login System (Z-RSA)

The project in the reviewed article [10] is regarding a secure web browser login system by implementing Zero-Knowledge Proof and Rivest, Shamir, and Adleman (RSA) algorithm. During the implementation, the algorithms will be used to prove whether a user know the password by sending hashing password to the server for verification purpose. Hence, the systems have no credentials or password to be compromised by storing on the server. Meanwhile, the system has fulllfil the criteria of zero-knowledge proof, including completeness, soundness, and zero-knowledge. It shows that the user can be verified successfully if he or she can provide a valid password hash, and vice versa. Besides, the server which acts as a verifier will not know the detail of a password via the hashing using one-time token.

Unlike the common login system which hashes the password using a Javascript-based MD5 and SHA algorithm before storing in a database, the proposed work in the reviewed article – Z-RSA creates a framework with the ASP.net, which can implement the Zero-Knowledge Proof Authentication. The core idea of the system is by hashing the password using a one-time token to form a signature. After that, the server will verify the signature, directly eliminating the need to transmit passwords or hashes over the network. In overall, the security and confidentiality of the web-based applications has been enhanced from the aspect of authentication process.

In overall, the utilization of one-time tokens prevents a similar value from being transmitted over the network. It indicates that the information or signature sent over the network will only be valid for once, hampering the effort of hackers to intercept the message. Other than that, it also prevents the password hashes or plaintext passwords from being sniffed. Even though the signature constructed from the hashing operation is sniffed by malicious hacker, the attacker will not be able to crack the plaintext password of the user.

Strengths and Weaknesses

Since the system in reviewed article has adopted RSA for ZKP, there is no credentials or password are going to be compromised by storing on the server. The password hashing will be implemented using a one-time token to form a signature, meanwhile the server will perform verification on the generated signature. Besides, the one-time token used for password hashing is only valid for once. Therefore, the overall security level has been further improved. Since the signing and verification operations are kept implementing, the computational cost is highly consuming even though it is manageable for current computing devices.

Table 4.1: Comparison table between ZKP Network Authentication, and Zero Knowledge Protocol with RSA Cryptography Algorithm for Authentication in Web Browser Login System (Z-RSA)

	ZKP Network Authentication	**Zero knowledge protocol with RSA Cryptography Algorithm for Authentication in Web Browser Login System (Z-RSA)**
Better security	✔	✔
Higher computational cost	✔	✔
Private Key Recoverability	✔	

Chapter 3

System Methodology/Approach

The project phases follow the Software Development Life Cycle (SDLC) framework. Each stage of the framework will be discussed in detail. The tools and the implementation challenges are stated below. Furthermore, the proposed timeline is presented using a Gantt chart.

3.1 Methodologies and General Work Procedures

The SDLC defines a framework to develop software within the schedule systematically. It comprises six phases: requirement gathering and analysis, design, development, testing, deployment, and maintenance. Following the standard allows the developer to develop the system systematically and increase overall efficiency.

High-quality software can be produced within schedule and estimated cost by following the phases provided in the framework. The testing will be conducted on every end of the stage to ensure output quality, reducing the time and cost of rework. In addition, the project risk is further reduced with detailed planning before implementation. Furthermore, the client will also be involved in the phases to perform requirement verification in each stage.

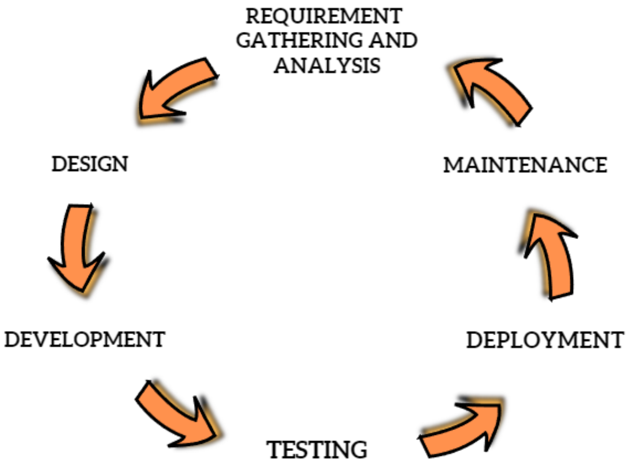


Figure 4.1: Software Development Life Cycle

3.1.1 Requirement Gathering and Analysis

The phase is separated into two main components: requirement gathering and requirement analysis. Since the project does not involve end-users, online research and reference to the journal articles were done to understand the problem statements of traditional network authentication and monitoring. Other than that, the project's objectives should be defined to have precise direction on the solution proposed. For this project, the goals established are the implementation of network authentication using the ZKP via RSA authentication scheme. Hence, the relevant core knowledge is required to plan project implementation.

On the other hand, the requirement analysis checks whether the product development is feasible. Hence, the project supervisor will be consulted to acquire the opinions from professionals. After that, the requirement gathered is adjusted according to the suggestions the project supervisor gave. Since the requirements are confirmed, they will be written into a proposal for the future reference of both developers and clients. In the proposed project, the requirements involved are all traffic will be intercepted by the proxy server, and each web request will be checked by the proxy server to validate if the relevant user has been authenticated themselves via the session record in connected database. If the user is not authenticated, redirecting the unauthenticated user to the captive portal when trying to browse other HTTP websites. Besides, the users are required to upload a private key private enhanced mail (PEM) in the captive portal to construct a signature, which will be then verified by the proxy server. Once users are authenticated, a session will be established, and the user IP address will be recorded for checking the authentication state. Once the IP address is valid, the proxy server will validate the user as an authenticated user and he or she is allowed to access Internet resources.

3.1.2 Design

For the design phase, the requirements collected in the previous stage will be applied to the system flowchart and the timeline schedule. Throughout the project, two flowcharts will be designed for separate operations, separated into ZKP network authentication and network monitoring. The first design focused on ZKP network authentication, which primarily involves user registration, authentication and granting network resources. Meanwhile, the second design focused on network monitoring includes capturing the resources parameter of proxy server and performing monitoring on the resource's usage.

Furthermore, the next component that should be involved in the design phase is the project timeline schedule. First, the project milestones should be broken, and the critical tasks of the project should be identified to avoid project delay. Throughout the project, the first milestone is developing a network authentication scheme using the ZKP protocol, which can be further broken down into smaller and manageable tasks. They include the selection of the ZKP technique, selecting tools for ZKP implementation, and the execution and testing of the ZKP authentication scheme. The second milestone of the project is installing the Zabbix server on Ubuntu virtual machine, capturing the resource usage of the proxy server and displaying in a dashboard.

3.1.3 Development

The tools, including hardware and software, should be prepared to start the development. The leading software in the project included is Ubuntu virtual machine, Visual Studio Code and Zabbix, while the hardware involved is a laptop and network-embedded devices such as Cisco Router 1841 and Cisco Catalyst 2960. The setups and configurations are required to smoothen the task implementation progress.

First, the coding of a captive portal will get started using Visual Studio Code. The user registration and authentication logic related to ZKP implementation will be included in the coding. The testing phase can be conducted simultaneously with the implementation phase. A web browser is needed to access the local website to test the server code after the proxy setting of the testing machine has been configured into proxy server's IP address and port number. Furthermore, a proxy server is hosted in the local area network, and all the traffic will go through the proxy server created using Node.js library. At the initial stage of connecting to a network, the unauthenticated user is not able to surf any HTTP website and they will be redirected into a captive portal. The users are forced to authenticate themselves by uploading their own employee ID and private key PEM file and submit it. Then, the client browser will perform a signing operation on a random challenge to construct a signature and send to the server for verification purpose.

Next, the network monitoring part requires Zabbix to empower the implementation. The steps can be started by installing the Zabbix server, installing Zabbix agent to capture the resource data, followed by displaying the information such as server health information on the dashboard.

3.1.4 Testing

The phase will be conducted at the end of every cycle. Furthermore, the simulation of the scenarios in ZKP registration and authentication is undertaken in the captive portal. However, the test users must be created, and the test scenarios must be launched in the captive portal. The captive portal testing test results are monitored and logged for future reference. In the project, it is assumed that an organization are having two databases, including human resource (HR) database, and captive portal database. The test users will be created on the HR database and assumed that they are already been reviewed by the HR personnel. For captive portal database, a new user will be created via the registration on the captive portal if the information provided by user is valid after comparing with the HR database.

From the perspective of network monitoring, it is ensured that the installation of Zabbix server, Zabbix agent, mySQL, Apache have been completed successfully. Then, the HTTP Apache website can be accessed to further view the dashboard and interpret the relevant resource usage.

3.1.5 Deployment

Before the product deployment, user acceptance testing (UAT) should be conducted to fit the expected results of the clients or end users. Nevertheless, the project does not involve the end users, so the team member will execute the UAT from the end users' perspectives. Since the UAT should be the replica of the production environment, the hardware, such as Cisco Router 1841 and Cisco Catalyst 2960, can be set up for testing. The expected result of the project is included that the users can browse HTTP websites after they are authenticated themselves via the captive portal. After the expected result is met, the product will be ready for demonstration and deployment.

For network monitoring, the dashboard of Zabbix server will be shown to the end user and adjust according to their requirement. It is to ensure that the end user who is a network administrator can gain the insights which can assist in resource usage of components within local network.

3.1.6 Maintenance

In future, the products deployed will require maintenance from time to time to ensure consistent quality. For network authentication, it is planned that to further enhance the security level of RSA authentication scheme applied in the captive portal. Besides, it is also essential to take initiative to reduce the communication cost of network authentication, which indicates the bandwidth usage and latency of transmitting the encrypted data.

Other than that, other Zabbix features could be added into system from time to time according to the requirements of the network administrators, providing the best user experience and insights. Next, the trigger and alert event should be configured so that the network administrator will get notified when there is any event that is exceed the configured threshold.

Chapter 4

System Design

4.1 Granting/Denying Network Access

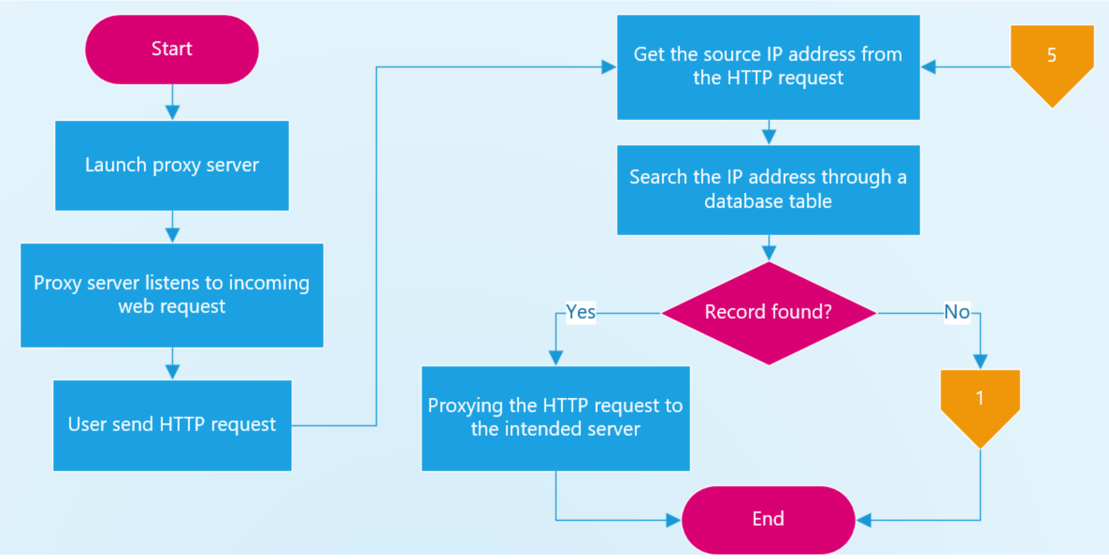

Start
Launch proxy server
Proxy server listens to incoming web request
User send HTTP request
Get the source IP address from the HTTP request
5
Search the IP address through a database table
Record found?
Yes
No
Proxying the HTTP request to the intended server
1
End

Figure 3.1: HTTP Proxy Logic

First step to activate the program is launching HTTP proxy server. After that, the proxy server will listen to incoming web request originating from HTTP protocol. Whenever user has sent a HTTP request, the proxy server will intercept the HTTP request and obtain its source IP address. Next, the proxy server will browse through the session table of captive portal database. If a valid record is found, the HTTP request will be proxied to the intended destination server, accessing the network resources. Else, the user will be redirected to the captive portal.

4.2 Captive Portal

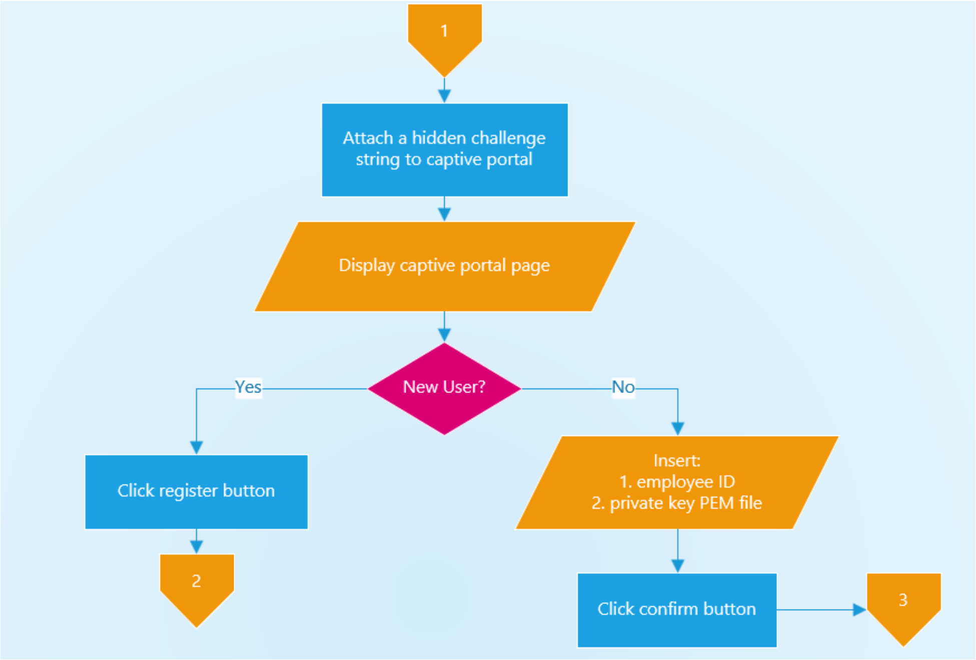


Figure 2.1: Captive Portal

The proxy server will generate a random generated string. Then, the random string will be rendered together with captive portal page as a hidden challenge value. Until the step above, the captive portal page has been displayed on client browser. Inside the captive portal, there are two fields which are required to fill in, including employee ID and private key PEM file. After filling up the form, the user can submit it and start the authentication process via RSA authentication scheme. If the users first time login into the captive portal or lost their key, the user shall access the registration page to register themselves or redownload the key.

4.3 User Registration

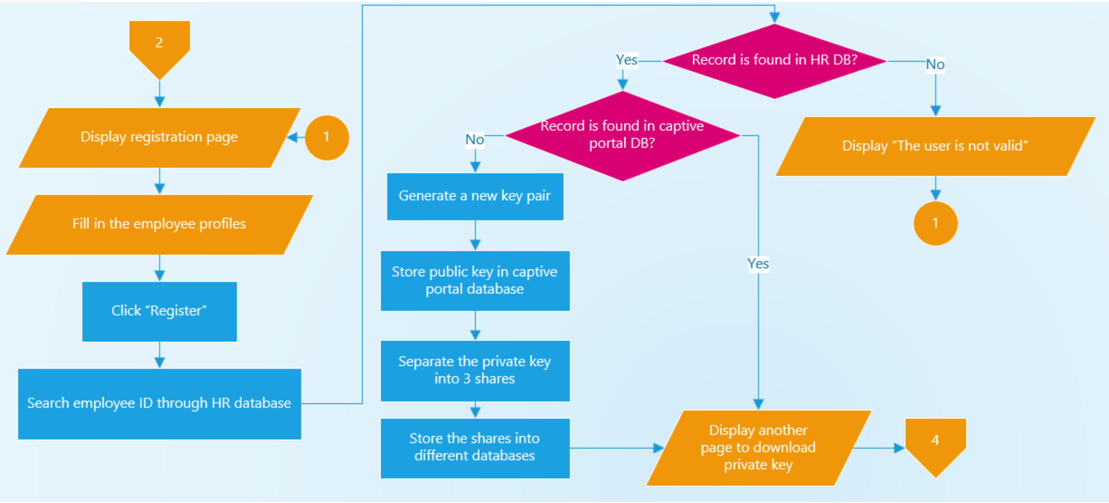

2
Display registration page
1
Fill in the employee profiles
Click "Register"
Search employee ID through HR database
Record is found in HR DB?
Yes
No
Record is found in captive portal DB?
No
Yes
Generate a new key pair
Store public key in captive portal database
Separate the private key into 3 shares
Store the shares into different databases
Display another page to download private key
4
Display "The user is not valid"
1

Figure 3.2: User Registration and Key Pair Generation

Once the user clicks on the register button, the registration page will be displayed on the client browser. The user is required to fill in the employee profiles or additional information which depends on the organization policy, proving that they are a valid user. After the user has submitted the registration form, the proxy server will browse through the human resource (HR) database to find a matched record, assuming that the HR database has been reviewed by the relevant personnel.

Furthermore, if there is a valid record in HR database, the proxy server will further browse through the captive portal database to know whether the user has been registered before. Else, the proxy server will generate a new key pair for the user. The public key PEM will be stored in the captive portal database, while the private key PEM will be splitted into three shares using concept of Shamir's secret sharing and stored in different databases, avoiding a single point of failure. If the user has registered before or gone through registration steps above, he or she will be redirected to another page, which mainly for recovering the missing private key.

4.4 Download Private Key PEM

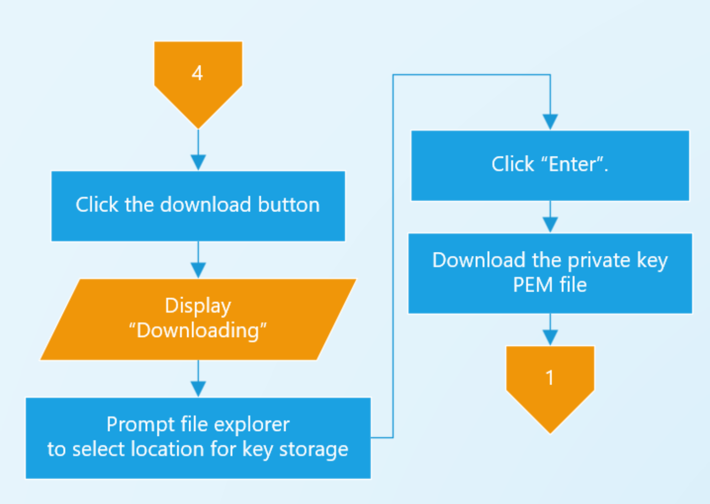

4
Click the download button
Display "Downloading"
Prompt file explorer to select location for key storage
Click "Enter".
Download the private key PEM file
1

Figure 3.3: Download of Private Key PEM File

Once the user has registered themselves, the user will be redirected to a page for downloading his or her private key. Once the user has downloaded the private key, he or she will be redirected back to captive portal.

4.5 User Authentication

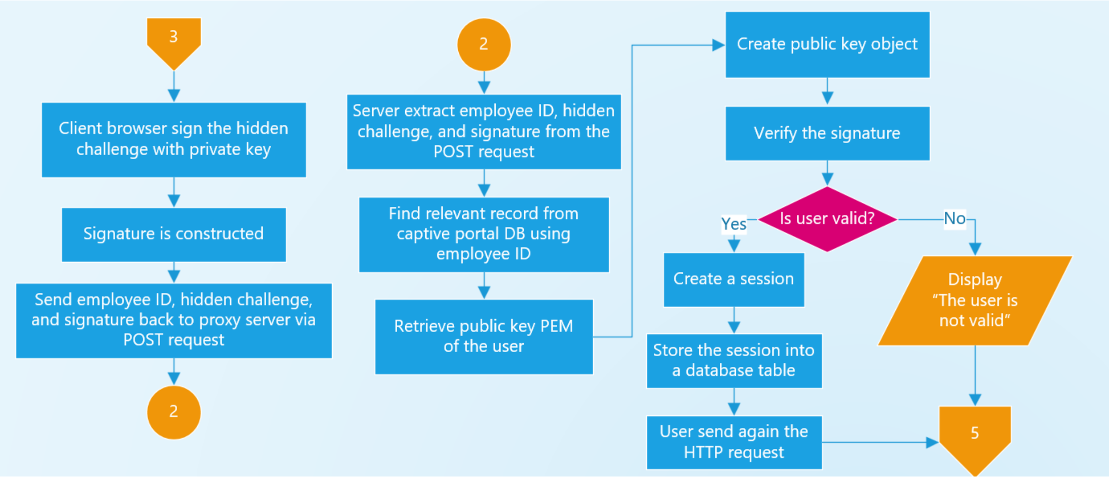

3
Client browser sign the hidden challenge with private key
Signature is constructed
Send employee ID, hidden challenge, and signature back to proxy server via POST request
2
2
Server extract employee ID, hidden challenge, and signature from the POST request
Find relevant record from captive portal DB using employee ID
Retrieve public key PEM of the user
Create public key object
Verify the signature
Is user valid?
Yes
No
Create a session
Store the session into a database table
User send again the HTTP request
Display "The user is not valid"
5

Figure 3.4: User Authentication

Once the user has submitted their employee ID and private key PEM file, the client browser will start to sign the hidden challenge value using client-side javascript. Once the signature has been constructed, the client browser will send a POST request to server regarding employee ID, hidden challenge, and signature for further processing. Since the signature construction is implemented at client side, it does not require user to surrender their private key throughout authentication process.

After the server has received the information, the server extracts the employee ID, hidden challenge value and signature from the POST request body. Next, the server will browse through captive portal database using employee ID and get public key PEM of respective user. The server will proceed with creating public key object using the public key PEM and perform verification process on the signature. If the user is proven to be valid, a session will be established and and stored in the session table of captive portal database. Before the session is expired, the user is allowed to access network resource by sending HTTP request.

4.6 Network Monitoring

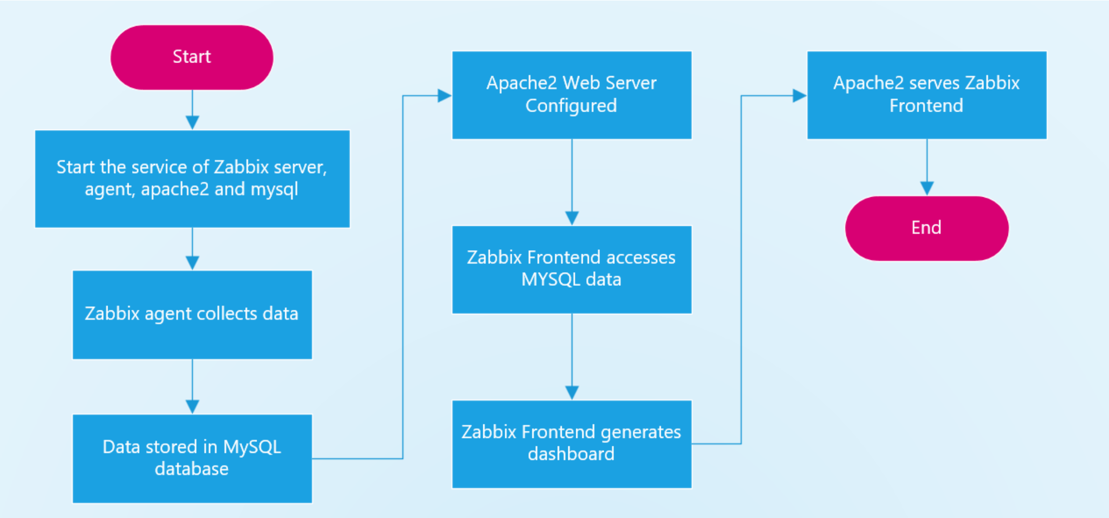

Start
Start the service of Zabbix server, agent, apache2 and mysql
Zabbix agent collects data
Data stored in MySQL database
Apache2 Web Server Configured
Zabbix Frontend accesses MYSQL data
Zabbix Frontend generates dashboard
Apache2 serves Zabbix Frontend
End

Figure 3.5: Generating Zabbix Dashboard

After the service of Zabbix Server, Zabbix Agent, Apache2 and MySQL have started, the Zabbix agent will collect data from the monitored hosts. Then, the data will be stored in MySQL database and the configuration of Apache2 web server is done. The Zabbix Frontend will start to access MySQL data and generate dashboard. Lastly, Apache2 will serve the Zabbix Frontend.

Chapter 5

System Implementation

5.1 Hardware Setup

The hardware involved in this project includes a laptop and network embedded devices such as the Cisco Router 1841 and Cisco Catalyst 2960. The laptop is used to launch software required to integrate with the Cisco Router 1841 for the implementation of the ZKP authentication scheme. The network embedded devices are used to build a platform for testing and simulating real-world networking scenarios in a controlled environment.

Table 8.1: Specifications of laptop

Description	Specifications
Model	ASUS Vivobook 14 M413IA
Processor	AMD Ryzen 5 5500U
Operating System	Windows 10
Graphic	AMD Radeon Graphics 2.10 GHz
Memory	8GB RAM
Storage	512GB SSD

Table 8.2: Specifications of Cisco Router

Description	Specifications
Model	Cisco 1800 Series Router: Cisco 1841
Product type	Modular Router
DRAM memory	256 MB
Flash memory	64 MB
Data link protocol	Ethernet, Fast Ethernet
Network/Transport Protocol	IPSec
Remote Management Protocol	SNMP, HTTP, SSH-2

Table 8.3: Specifications of Cisco Switch

Description	Specifications
Model	Cisco Catalyst 2960 Series
Forwarding bandwidth	16 Gbps
Switching bandwidth	32 Gbps
Flash memory	32 MB
DRAM	64 MB
Maximum Transmission Unit	Up to 9000 bytes
Maximum Forwarding Rate	6.5 Mpps

5.2 Software Setup

For the software setup, Ubuntu 20.04.6 LTS is one of the widely used distribution of Linux, which consists of a strong community support. It will be configured to host the proxy server for testing purpose. Meanwhile, the Visual Studio Code is a source code editor which is the main platform in editing server source code and launching the server. Lastly, Zabbix is an open-source network monitoring tools, enabling the monitoring, and tracking of server health condition. The Zabbix Frontend will be used to visualize the dashboard after the Zabbix agent collected the data from the monitored devices. Lastly, MySQL will serve as database backend and Apache will serve as web server to support Zabbix Frontend.

Table 9.1: Ubuntu Operating System

Operating System	Ubuntu 20.04.6 LTS
Codename	Focal Fossa
Memory	4 GB
Virtual Size Allocated	20 GB
Network Adapter	Intel® Wi-Fi 6 AX200 160MHz

	(Attached to Bridged Adapter)

Table 9.2: Visual Studio Code

Version	1.65.2
Node.js	14.16.0
Operating System	Windows_NT x64 10.0.22631

Table 9.3: Zabbix

Zabbix Version	6.0 LTS
OS Distribution	Ubuntu
OS Version	20.04 (Focal)
Zabbix Component	Server, Frontend, Agent
Database	MySQL
Web Server	Apache

5.3 Setting and Configuration

5.3.1 External Libraries

In the Node.js development environment, libraries required to be installed are as below:

a) **express:** A framework commonly applied for Node.js for web applications.

b) **body-parser**: To create a middleware which parses incoming request bodies in Express.

c) **NodeRSA**: Main library used in RSA cryptography in Node.js server.

d) **jsrsasign**: Main library being used in RSA cryptography in client browser for signing.

e) **http-proxy**: Main library to create a HTTP proxy server in Node.js.

f) **mongoose:** MongoDB object modeling tool.

g) **express-session:** Creating a middleware for session management in Express.

h) **connect-mongodb-session:** A session store mainly backed by MongoDB in Express.

5.3.2 MongoDB Atlas

a) Create an Account on MongoDB Atlas

b) Login into MongoDB Atlas account and view the dashboard.

c) Set up a cluster for the project purpose by following the required information.

d) Once the cluster is created, click on the “Collections” tab under the “Database” section.

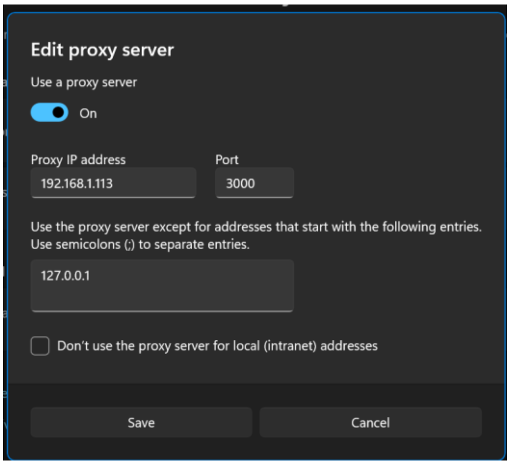
e) The database below is required to be created.
(i) HR_Database
(ii) Captive_Portal_Database
(iii) Private_Key_Database_01
(iv) Private_Key_Database_02
(v) Private_Key_Database_03

5.3.3 Proxy Setting on Client PC

a) Go to Settings – Network and internet – Proxy.

b) Go to “Manual proxy setup” section and click “Set up”.

c) Configure the proxy address according to setup environment.



Edit proxy server

Use a proxy server

On

Proxy IP address: 192.168.1.113

Port: 3000

Use the proxy server except for addresses that start with the following entries. Use semicolons (;) to separate entries.

127.0.0.1

☐ Don't use the proxy server for local (intranet) addresses

Figure 4.1: Edit Proxy Server on Client PC

5.3.4 Zabbix configuration

Note: The configuration commands can be found at Zabbix official website.

a) Zabbix server installation

b) Zabbix server, frontend, and agent installation

c) mySQL database creation

d) The initial schema and data are required to be imported on Zabbix server.

e) Disable the option "log_bin_trust_function_creators" after importing database schema.

f) Configure the Zabbix server's database configuration file.

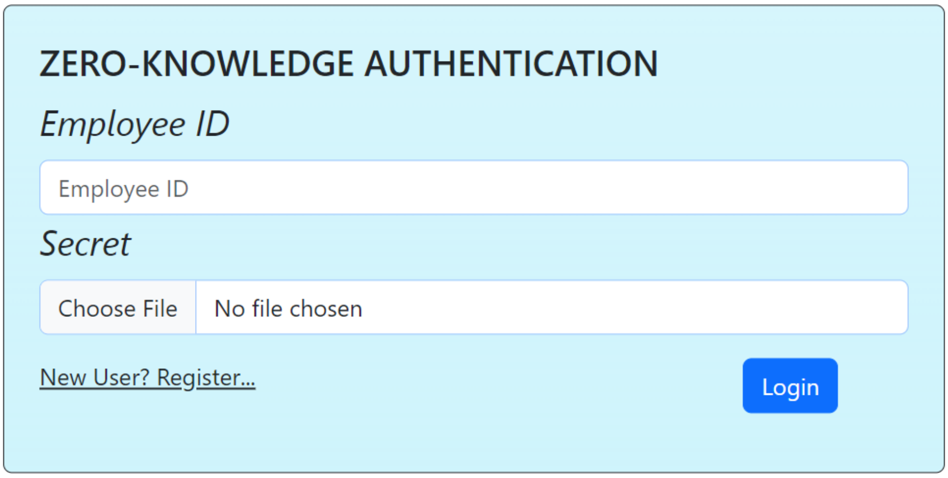
g) The respective processes of Zabbix server and agent are required to be started.

h) Enable the processes to be started once the machine is up and running.

i) Browse the Zabbix UI web page, which is http://<host_ip_address>/zabbix

5.4 System Operation

5.4.1 Captive Portal Page



ZERO-KNOWLEDGE AUTHENTICATION

Employee ID

Employee ID

Secret

Figure 5.1: Captive Portal Page

After the user connect to network and first time access the HTTP website, the user will enter the captive portal. The user can input their employee ID and upload their private key PEM file. After the user clicked **"Login"** button, the verification process will be started. If the user is new user, they shall click the **“New User? Register…”** button to access registration page.

5.4.2 Registration Page

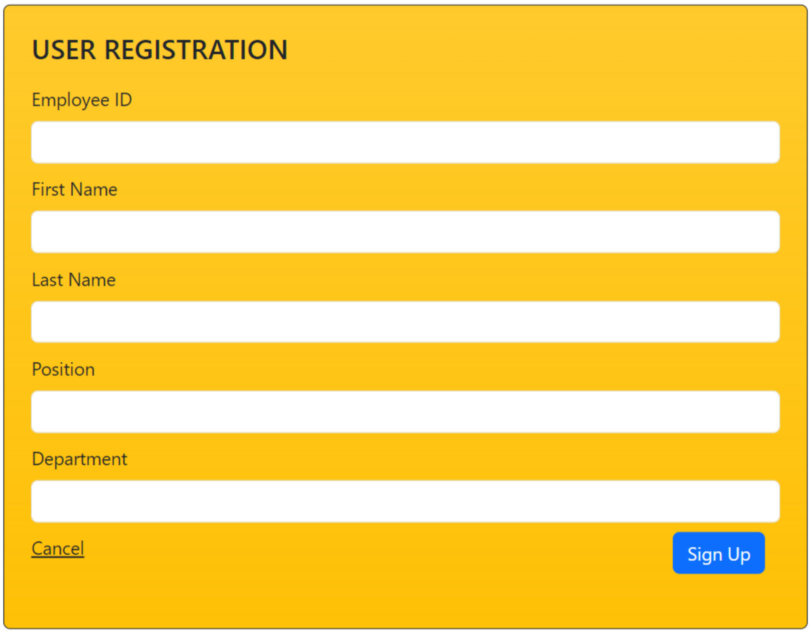
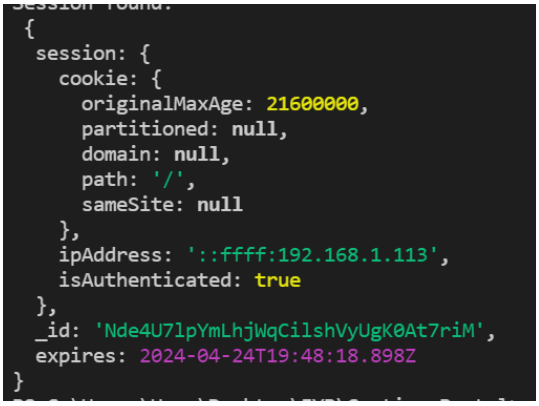


Figure 5.2: Registration Page

The new user can key in the information here to prove that he or she is a valid user. In this project, the submitted data will be compared with the HR database records which assumed that it has been verified by HR personnel. The information required to key in is depending on organization policy. For instance, the organization will assign an authentication token to every valid employee and use to prove own identity. The registration page can also be used to recover their lost private key by going through again the registration process.

5.4.3 Server Log Message – Successful Authentication



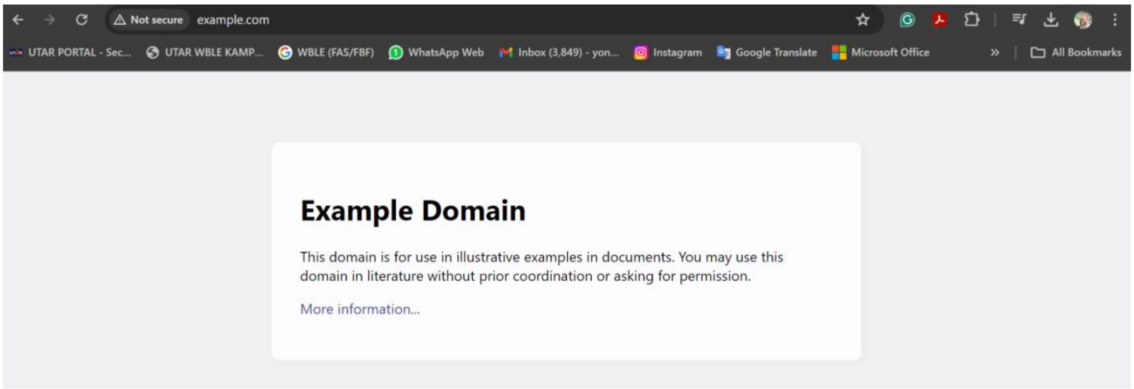
```
Session found:
{
  session: {
    cookie: {
      originalMaxAge: 21600000,
      partitioned: null,
      domain: null,
      path: '/',
      sameSite: null
    },
    ipAddress: '::ffff:192.168.1.113',
    isAuthenticated: true
  },
  _id: 'Nde4U71pYmLhjWqCilshVyUgK0At7riM',
  expires: 2024-04-24T19:48:18.898Z
}
```

Figure 5.3: Session Information after Successful Authentication.

Once the user has been successfully login, the session message will be displayed on the server log. Once the session has been established, the MongoDB will store a record and the respective user will be able to access HTTP resource.

5.4.4 Accessing the Network Resource

a) Authenticated User



Example Domain

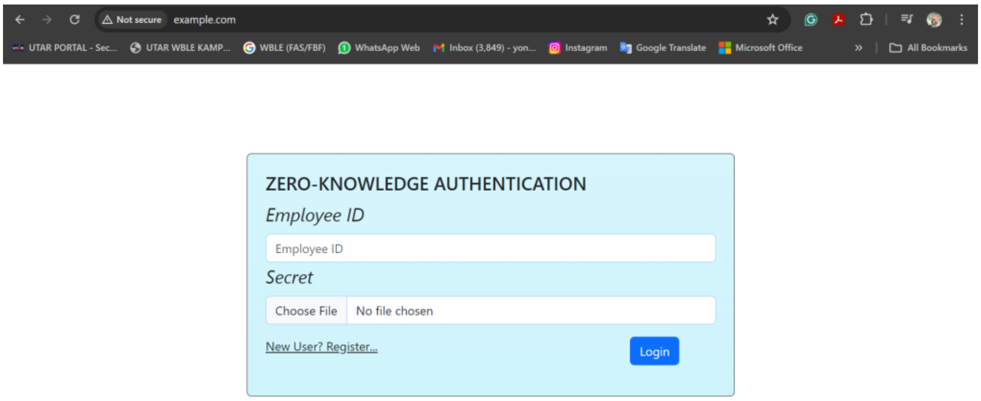
This domain is for use in illustrative examples in documents. You may use this domain in literature without prior coordination or asking for permission.

More information...

Figure 5.4: User Can Access HTTP Website after Successful Authentication

After the user authenticated themselves, he or she can access the network resources.

b) Unauthenticated User



ZERO-KNOWLEDGE AUTHENTICATION

Employee ID

Employee ID

Secret

Choose File No file chosen

Figure 5.5: User Cannot Access HTTP Website before Successful Authentication

Since the user is not authenticated, he or she will keep being redirected into captive portal and cannot access the network resources.

5.4.5 Network Monitoring via Zabbix Dashboard

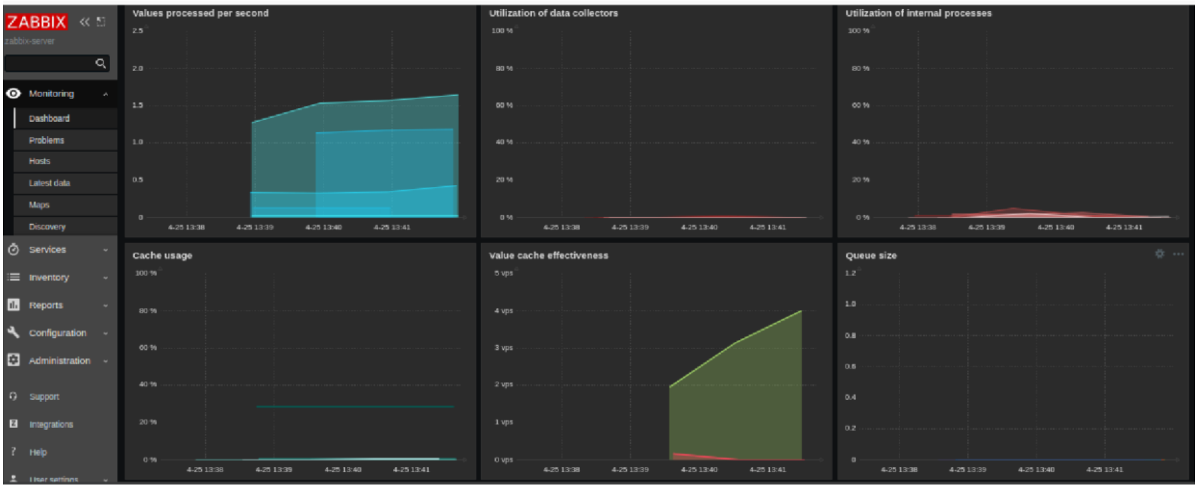


Figure 5.6: Zabbix Dashboard

From the Zabbix dashboard above, the network administrator can gain some insights regarding the network resource usage such as queue size and cache usage. The graphs will be updated from time to time according ot the data collected by Zabbix agent.

5.5 Implementation Issues and Challenges

5.5.1 RSA Library Selection

Due to the nature of public key cryptography, the private key is mandatory for users to keep securely. Hence, the signing operation of RSA authentication scheme is necessary to implement at the client side which is the client browser. However, some of the libraries are only supported the RSA operations on the server side, while some of them are only able to be operated over secure environment such as HTTPS website. Throughout project development, project team member only managed to establish a HTTP captive portal and allowed the user to engage in the interaction with the captive portal. Hence, there is a lot of time spent on RSA library selection. Eventually, it is found that jsrsasign library has supported the client-side RSA operation such as signing operation even under HTTP environment.

5.5.2 Integration Issue between Squid Proxy and Node.js Captive Portal

Initially, the proxy server to be applied in the project is Squid proxy. The trial of integrating the NodeJS captive portal and Squid proxy has failed, because the testing of captive portal is not performed to get expected result. The users are not able to be redirected to captive portal if the users have not authenticated themselves yet. As per observations above, there is a discussion with project supervisor, and it is agreed to develop proxy server and web server hosting the captive portal into a single component. After further research, it is possible to develop Node.js server which consist of two components which are proxy server and captive portal, via external Node.js library “http-proxy”. However, the project team member is only managed to develop a HTTP proxy due to limited knowledge on Secure Socket Layer (SSL) interception.

5.5.3 Difficulty in Finding Relevant Element in Maintaining State of Authentication

In the context of HTTP requests, domain represents the website’s domain name which is being accessed. Since the incoming HTTP requests could come from different domains, the only items that could be retrieved from the HTTP requests are source IP addresses. Hence, the IP address of user will be stored after the authentication and used for checking the authentication state. The state of being authenticated is by comparing the IP address inside the session records stored in the database with the source IP address of incoming HTTP requests.

5.5.4 Difficulty in Creating a HTTPS Proxy Server using Node.js

The challenge lies in implementing SSL bump using Node.js, specifically with MITM proxy and HTTPS proxy configurations. Attempts to trigger the HTTPS connect event have failed, likely due to inadequate online examples and insufficient documentation from the “http-proxy” library, causing confusion in implementation. Consequently, the solution has been limited to HTTP proxying rather than intercepting and modifying both HTTP and HTTPS requests and responses, restricting the ability to achieve desired functionalities.

5.6 Concluding Remark

Chapter 5 System Implementation has dived into the setup of various tools being utilised in the project. The hardware included such as Cisco Router 1841 and Cisco Catalyst Switch 2960 are needed to simulate the real-world environment. For software setup, there are multiple external libraries are required to be installed in the Node.js project directory. Besides, MongoDB Atlas is required to set up and performs as a key database throughout the project. Since the project is focused more on the authentication part, the web interface should be simple and user-friendly as per demonstrated in the system operation which consisted of user registration and user authentication page only. Throughout the implementation of project, there are multiple challenges being faced, leading to the stuck of project progress.

Chapter 6

System Evaluation and Discussion

6.1 System Testing and Performance Metrics

In this subsection, the comparison between username and password authentication and RSA authentication will be performed. The typical password length "n" adopted by most of the organizations is 8 characters. Besides, the possible characters from the keyboards "c" are 94 characters, including special characters, uppercase letters, lowercase letters and 10 digits in total. To calculate possible combinations of the characters via username and password authentication, the total number of possible combinations from characters from the keyboards based on the password length is as below:

If $n = 8$, $c = 94$, the possible combination of username/password authentication
$= c^n$
$= 94^8$
$\approx 6.095689 \text{ x } 10^{15}$

Even though the possible combinations of username and password authentication are considered immense, the possibility to be cracked is still there. By combining modern computing power and the skills required to write an automated script, the brute-force attacks can be an option in attempting a bunch of combination in a quicker mean.

Meanwhile, the factors deciding the strength of RSA authentication is large prime numbers and the computational complexity of product factor. RSA autthentication scheme has been widely adopted due to its maturity in terms of technology. Before diving into the calculation to show the possible combinations, each bits have two possibilities, either 0 or 1. In this project, the key size selected in the project is 2048 bits, which able to contribute a comparatively immense number of possible combinations.

The value of RSA possible combinations with key size 2048 bits

$= 2^{2048}$

$\approx 3.2317 \times 10^{617}$

As demonstrated above, the number of possible combinations in RSA authentication with a 2048-bit key size is more significant compared to the number of possible combinations in username and password authentication. Hence, high computational power and immense times of trials are required to crack the RSA authentication scheme and considered to be secure against the current capabilities of computing power.

6.2 Testing Setup and Result

By setting up the hardware and software, some testing has been conducted to further prove the reliability of the system. Besides, it can also validate the system functionality to see if it is able to meet the user requirements. As specified in the project scope earlier, the testing performed will only focused on HTTP websites.

6.2.1 HTTP Website 1 - http://example.com

Test Case 1 – User has authenticated successfully

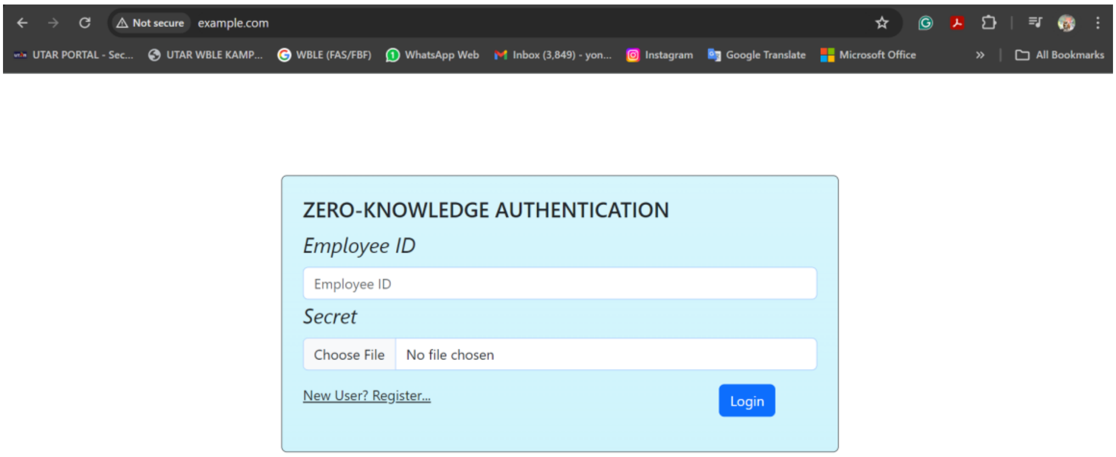
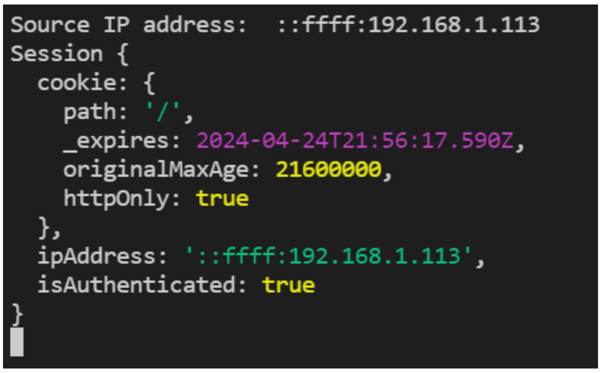


Figure 6.1: Captive Portal Page

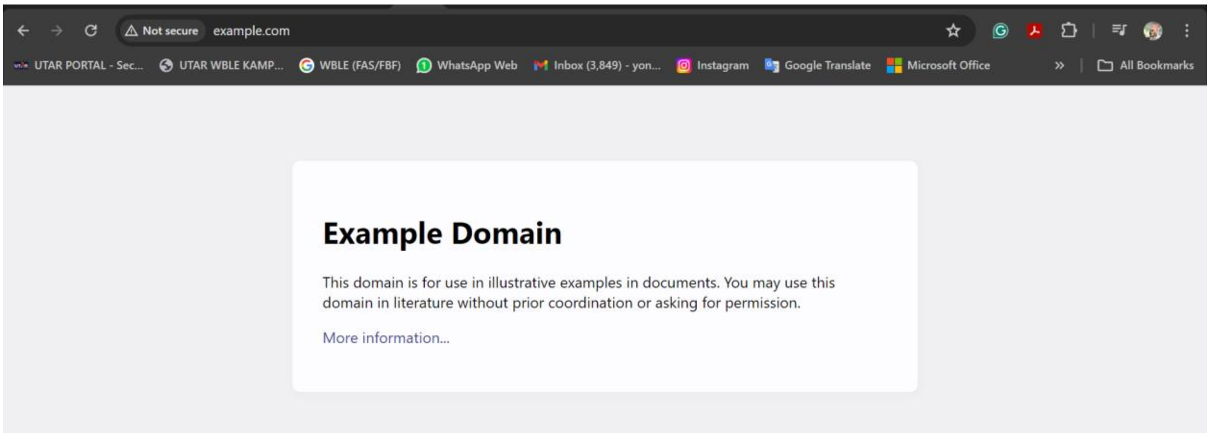
When user is unauthenticated, the user will be redirected into the captive portal to perform authentication.



```
Source IP address:  ::ffff:192.168.1.113
Session {
  cookie: {
    path: '/',
    _expires: 2024-04-24T21:56:17.590Z,
    originalMaxAge: 21600000,
    httpOnly: true
  },
  ipAddress: '::ffff:192.168.1.113',
  isAuthenticated: true
}
```

Figure 6.2: Session Information after Successful Authentication

Once the user authentication is performed successfully via captive portal page, the server will log the source IP address of user. After that, session has been established and a record will be stored in database.



Example Domain

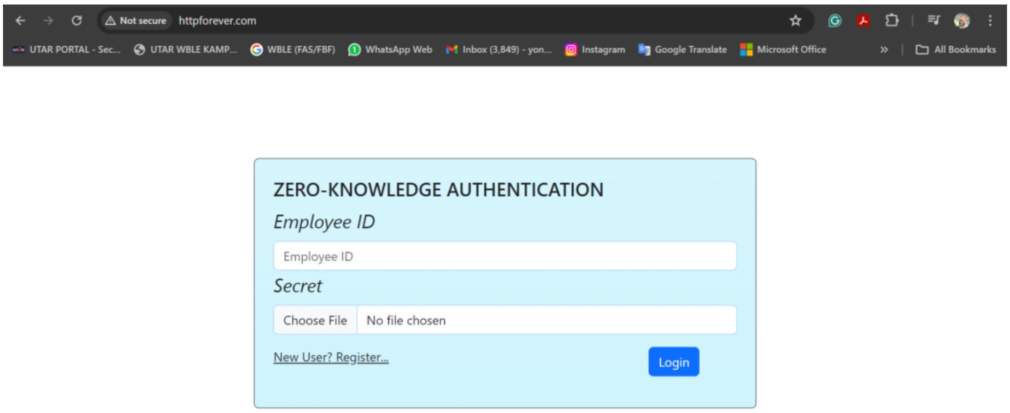
This domain is for use in illustrative examples in documents. You may use this domain in literature without prior coordination or asking for permission.

More information...

Figure 6.3: Access to HTTP Websites after Successful Authentication

After the user has been authenticated successfully, the HTTP website can be accessed after the user tried to refresh again the website.

Test Case 2 – User has failed to authenticate themselves



ZERO-KNOWLEDGE AUTHENTICATION

Employee ID

Employee ID

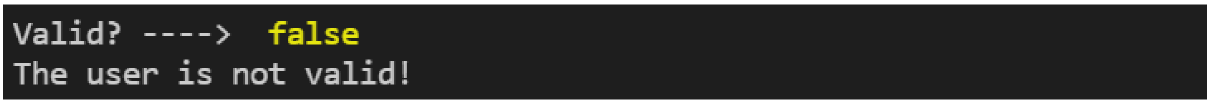
Secret

Choose File No file chosen

New User? Register...

Figure 7.1: Captive Portal Page

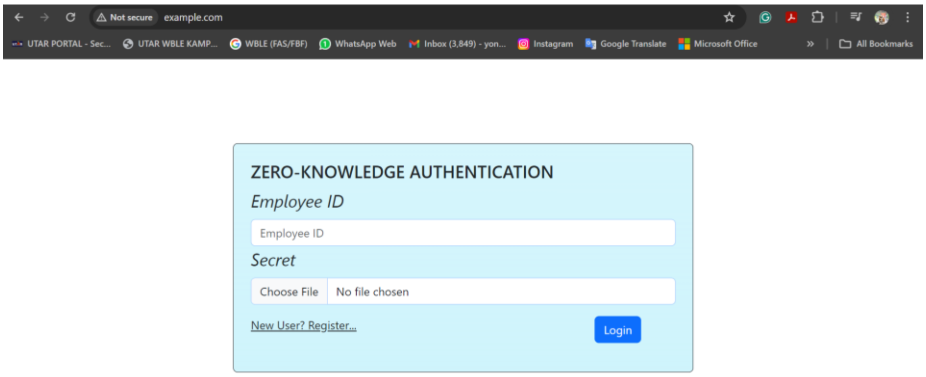
When user is unauthenticated, the user will be redirected into the captive portal to perform authentication.



```
Valid? ---->  false
The user is not valid!
```

Figure 7.2: User Authentication Failed

Once the user authentication is failed to perform, the server will log the message indicating that the user is not valid.



ZERO-KNOWLEDGE AUTHENTICATION

Employee ID

Employee ID

Secret

Choose File No file chosen

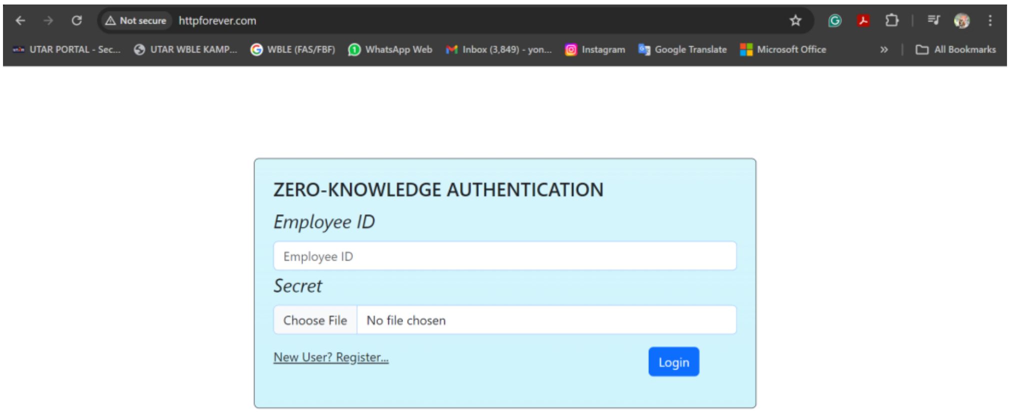
New User? Register...

Figure 7.3: Captive Portal Page

Even when the user tried to refresh the page, he or she will still redirect into the captive portal.

6.2.2 HTTP Website 2 - http://httpforever.com

Test Case 1 – User has authenticated successfully.



ZERO-KNOWLEDGE AUTHENTICATION

Employee ID

Employee ID

Secret

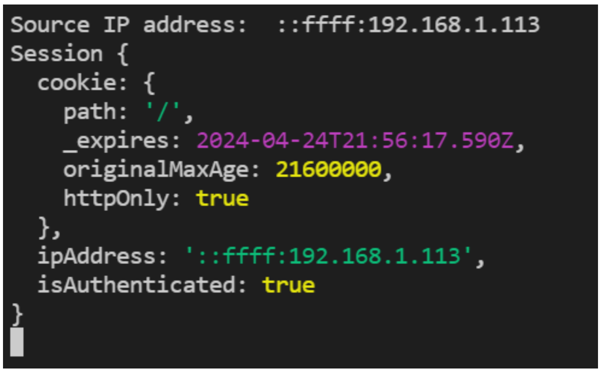
Choose File No file chosen

New User? Register...

Login

Figure 8.1: Captive Portal Page

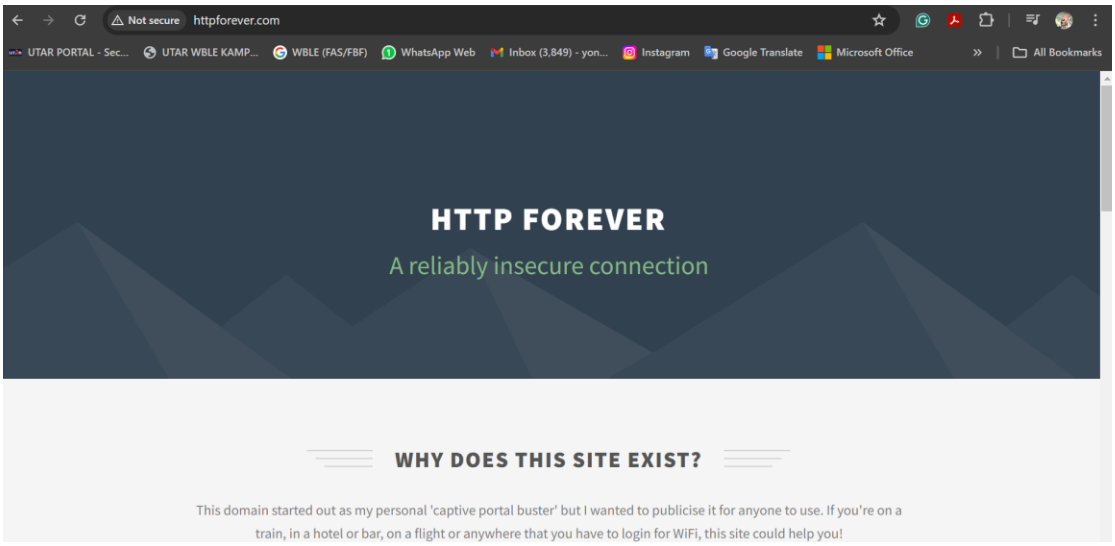
When user is unauthenticated, the user will be redirected into the captive portal to perform authentication.



```
Source IP address:  ::ffff:192.168.1.113
Session {
  cookie: {
    path: '/',
    _expires: 2024-04-24T21:56:17.590Z,
    originalMaxAge: 21600000,
    httpOnly: true
  },
  ipAddress: '::ffff:192.168.1.113',
  isAuthenticated: true
}
```

Figure 8.2: Session Information after Successful Authentication

Once the user authentication is performed successfully, the server will log the source IP address of user. After that, a session will be established and a session record will be stored in database table.



HTTP FOREVER

A reliably insecure connection

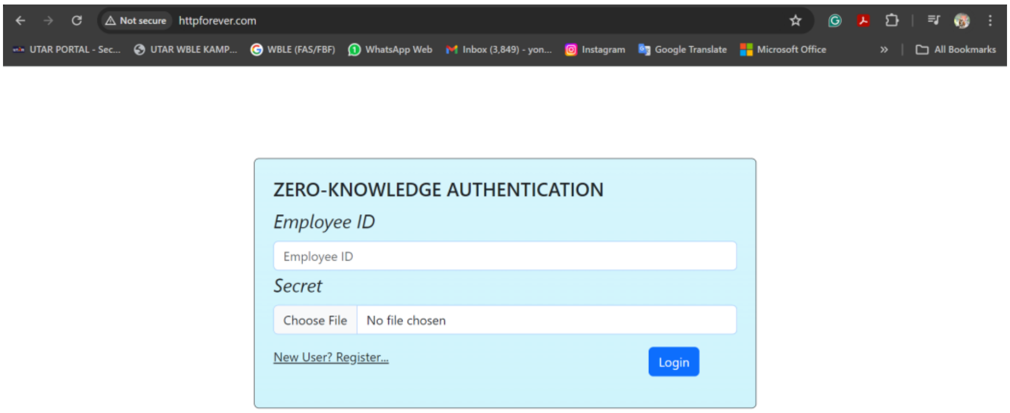
WHY DOES THIS SITE EXIST?

This domain started out as my personal 'captive portal buster' but I wanted to publicise it for anyone to use. If you're on a train, in a hotel or bar, on a flight or anywhere that you have to login for WiFi, this site could help you!

Figure 8.3: Access to HTTP Websites after Successful Authentication

After the user has been authenticated successfully, the HTTP website can be accessed after the user tried to refresh again the website.

Test Case 2 – User has failed to authenticate themselves.



ZERO-KNOWLEDGE AUTHENTICATION

Employee ID

Employee ID

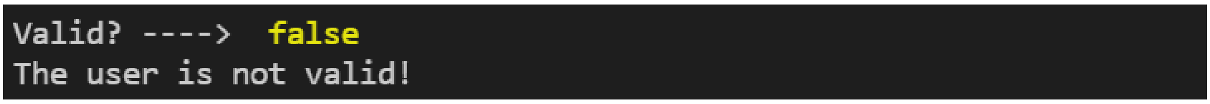
Secret

No file chosen

New User? Register...

Figure 9.1: Captive Portal Page

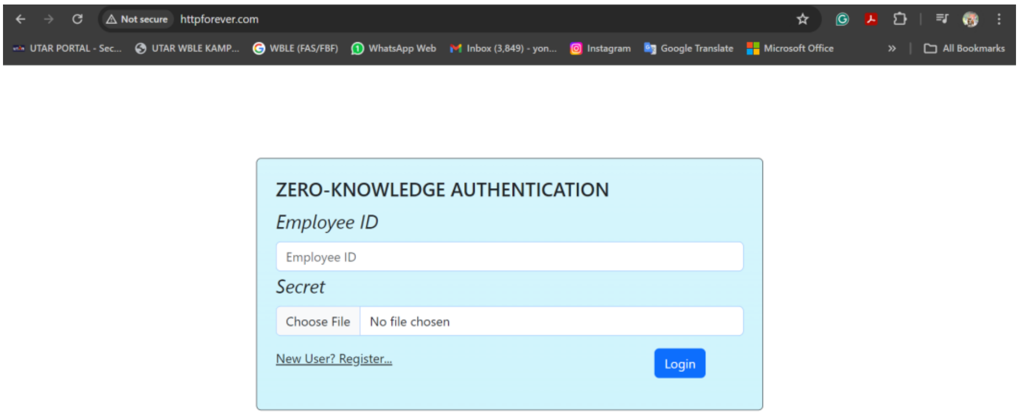
When user is unauthenticated, the user will be redirected into the captive portal to perform authentication.



```
Valid? ---->  false
The user is not valid!
```

Figure 9.2: User Authentication Failed

Once the user authentication is failed to perform, the server will log the message indicating that the user is not valid.



ZERO-KNOWLEDGE AUTHENTICATION

Employee ID

Employee ID

Secret

Choose File No file chosen

New User? Register...

Login

Figure 9.3: Captive Portal Page

Even when the user tried to refresh the page, he or she will still redirect into the captive portal.

6.3 Project Challenges

6.3.1 Scope Management

Initially, the project is separated into two major domains, which are network authentication and network monitoring. Hence, the research of both areas is being conducted at the same time, causing the overflow of information. It indirectly consumes majority of time in doing the online research and feels insecure to start implement due to insufficient studies being made. As per discussed with the project supervisor, the project scope has been more focused towards the network authentication compared to network monitoring. It relieves the huge workload on the project by putting majority focus on the network authentication using RSA authentication scheme to realize the ZKP network authentication.

6.3.2 Time Management

Since there are multiple festivals happened in January 2024 trimester, the project schedule has been delayed due to numerous days of public holidays. Other than that, the implementation stage has prompted different challenges, and the project member could only keep trying and seek potential solutions to solve such challenges. It indeed causes a serious problem due to the delay in project schedule and delay in meeting the project milestones because it is quite time consuming to debug the issue confronted one by one. At the end, the project objectives and scopes must be minimised to a level which can be managable, so that the project can meet the schedule at the right time.

6.4 Objectives Evaluation

6.4.1 Objective Recap

The objective of the project is aiming to integrate the ZKP authentication into network authentication process, so that the user can prove themselves as a valid user without compromising any sensitive information. To implement the authentication scheme, the external libraries such as NodeRSA and jsrsasign have been imported to facilitate the RSA authentication implementation. Those libraries are involved in RSA key pair generation, signing, and verification processes with their own custom functions or modules. By streamlining the overall process in ZKP implementation, the proposed system in the project can implement the ZKP authentication successfully for network authentication purposes.

6.4.2 Evaluation Criteria

The proposed system is evaluated to be more secure by comparing the possible combination from RSA and username and password authentication, which has been discussed in the subsection 6.1. The 2048-bit of RSA authentication key is more secure compared to username and password authentication, as there is an immense gap of possible combinations between RSA authentication and username and password authentication. Hence, more computational resources are needed to break through the RSA encryption for current stage.

Furthermore, the proposed system has integrated the ZKP technology in network authentication successfully. For instance, the proxy server created in the proposed system can allow or deny the HTTP traffic according to the user's authentication state. Once the user has been authenticated themselves via captive portal, the user's HTTP request will be proxied to the HTTP destination server as usual.

6.4.3 Strengths and Weaknesses

The proposed system's strength is more on the utilization of 2048-bit RSA key. It enhances the possible number of combinations, causing the signing and verification of RSA authentication scheme more complex. Hence, the level of difficulty to be cracked via brute-force attacks has been heightened, requiring more effort to find a vulnerability on the RSA authentication scheme.

Other than that, the key management can be more flexible in terms of private key storage. In this project, the private key recoverability has been emphasised due to the nature of human which easily forgots the location of storing the key or the key is being accidentally deleted and so on. At the same time, the project has adopted a mean to store private keys which separate the private key into different pieces and store them in different databases, reducing the possibility or impact caused by key compromise incidents.

For the weaknesses, the system is lacked the ability to monitor the HTTPS web requests because it is not capable of intercepting HTTPS traffic. Nowadays, most of the websites are adopting HTTPS protocol in web request since HTTPS provides more security via data encryption in transit. In case the system is not able to intercept the HTTPS traffic, it is not possible for the proxy server to have proxying into the intended destination server, limiting the practical use cases.

Other than that, the 2048-bit of RSA key sizes might be cracked easily in the coming future, due to the continuous growth trend in the computational power for devices. When the computational power keeps advanacing, the malicious attacker can have higher chance to crack over the key easily. However, the key size of RSA authentication scheme can be adjusted to enable more RSA key combination, further requiring more computational power to crack the RSA authentication scheme.

6.5 Concluding Remark

To summarise Chapter 6, the performance of the system has been assessed and tested with the number of possible combinations between RSA authentication and username and password authentication. With the figures of possible combinations demonstrated above, it is proven that RSA authentication provides more security level. There are test cases for two different HTTP websites, mainly from the perspective of unauthenticated user and authenticated users, to ensure that the system is working as expected and validate the system requirement. However, there are some project challenges being raised throughout the project period, including scope management and time management. Scope management involves the change of focus area in the project, focusing more on the network authentication as compared to network monitoring. Meanwhile, time management also discusses further on the potential reasons affecting the project schedule and timeline of delivering project milestones. Next, the integration of ZKP authentication into network authentication process has been implemented, enabling a valid user to authenticate himself or herself without compromising any sensitive information. Furthermore, the proposed system can integrate ZKP technology in network authentication, allowing proxy to manage HTTP traffic according to user’s authentication state. By performing strengths and weaknesses analysis, the system’s strengths and weaknesses have been identified. The strengths of the system have included more possible number of combinations as well as flexibility in managing key pair of RSA authentication scheme. The flexible mean in storing the key pair enables private key recoverability while separating key into multiple pieces and storing into different databases. By viewing from another perspective, the system is unable to intercept HTTPS traffic, lacking the ability to proxy the request to an intended HTTPS destination server even if the user has been authenticated, limiting its use case in real-world situation. Finally, the growing trend of computational power for devices are considered a threat for the system. It is because that the attackers can attempt more combination at a time, shortening the time required to crack RSA authentication scheme.

Chapter 7

Conclusion and Recommendation

7.1 Conclusion

The project has addressed the weakness in password security via the implementation of the ZKP authentication in network access. Other than that, the single point of failure in database storage can be refrained by separating the private key into pieces and storing them into different databases. Meanwhile, it enables the private key recoverability even though the private key must be surrendered and stored at the server. However, when it comes to real-world implementation, those server data would have another layer of encryption to ensure adequate level of security. The direction and scope for the project has been divided into two parts, which are network authentication and network monitoring. However, majority of the project will emphasis more on the network authentication. The core implementation of the project is to apply RSA authentication scheme for signing, verification, and key generation purpose. A captive portal will be constructed and hosted locally to conduct testing for network authentication process. The proxy server will keep checking source IP address of incoming HTTP requests and perform comparison with the session records stored in database. At the same time, ZKP will not be included in the implementation of network monitoring, focusing on dashboard display of Zabbix server. There are seven articles being reviewed in total, and the strengths and weaknesses for different articles have been highlighted. In overall, the proposed system in this project is having better security level, manageable for the common computing devices to handle cryptographic operations, as well as ensuring the private key recoverability.

In this project, the project phases follow the Software Development Life Cycle (SDLC) framework. The SDLC framework comprises of six phases from requirement gathering and analysis, until maintenance phase. For the overall flow of system, it is started by HTTP proxy logic. When the user has authenticated themselves and a session record has been stored in the database, the user will be able to access the HTTP resource. If the user is not being authenticated yet, it will redirect to captive portal. Then, the user will need to submit their employee ID and private key PEM file and proceed the authentication processes using RSA authentication scheme. If user is verified to be valid, a session will be created and stored in MongoDB. After that, the user can access to HTTP request until the session is expired. In case the user is a new user, it is required for the user to register themselves via the registration page first. The user can still recover his or her private key if it is accidentally deleted by going through the registration process again.

Visual Studio Code, MongoDB Atlas, and Zabbix would be the key tools being applied in the project implementation. By benchmarking username and password authentication and RSA authentication via possible number of combinations, it is proven that RSA authentication provides more combinations, and it required more computational efforts to crack the RSA encryption. By implementing the test cases, the system can integrate ZKP technology in network authentication, allowing proxy to manage HTTP traffic according to user’s authentication state. After that, the strengths and weaknesses of the system has been assessed from different perspectives. Firstly, the system allows more possible number of combinations as compared to username and password authentication, heightening the security level of system. Furthermore, the flexibility of managing key pair in RSA authentication scheme allows to separate the private key into pieces and store into different databases, ensuring that the private key can be recovered. Nevertheless, the HTTPS traffic could not be intercepted by the system, lacking the ability to proxy the request to intended HTTPS server. Furthermore, the computational power for computing devices is growing rapidly, which can be considered as a threat for the system by reducing the computational efforts to crack RSA encryption.

7.2 Recommendation

The recommendation which could be further enhanced the system is replacing RSA algorithm with Elliptic Curve Cryptography (ECC) algorithm. ECC algorithm provides identical level of security as RSA algorithm in a smaller key size. For example, 256 bits of ECC key can provide identical level of security with RSA key of 3072 bits. Due to the mathematical properties of ECC, it is more robust to against multiple types of cryptographic attacks. Therefore, ECC could be one of the future-proof solution to against attackers along with the growth of computational power.

Other than that, HTTPS proxy should be implemented so that the system could intercept the web requests from both HTTP and HTTPS. The proposed system in the project is developed using Node.js. However, the online documentation regarding the proxy implementation could be limited and it is required more development effort. By viewing from opposite side, the system could have more flexibility to manage the key pair, so that we can store pieces of private key in separate databases. It could ensure the private key recoverability and avoid single point of failure in storage side if there is any unauthorized access. Lastly, there are also multiple open-source proxy software available in the market, including Squid and pfSense. In short, the development of the system could be either using Node.js or those open-source proxy, depending on the organization demands.

REFERENCES

[1] M. O’Connor, “What is Passwordless Authentication?,” *RSA*, Jun. 10, 2021. https://www.rsa.com/resources/blog/passwordless/what-is-passwordless-authentication/ (accessed Apr. 20, 2024).

[2] “Resecurity | Cyber Attacks on Data Center Organizations,” *www.resecurity.com*, Feb. 20, 2023. https://www.resecurity.com/blog/article/cyber-attacks-on-data-center-organizations (accessed Apr. 04, 2023).

[3] “What is Shamir’s Secret Sharing?,” *Ledger*. https://www.ledger.com/academy/topics/security/shamirs-secret-sharing (accessed Apr. 25, 2024).

[4] N. Xi, W. Li, L. Jing, and J. Ma, “ZAMA: A ZKP-Based Anonymous Mutual Authentication Scheme for the IoV,” *IEEE Internet of Things Journal*, vol. 9, no. 22, pp. 22903–22913, Nov. 2022, doi: https://doi.org/10.1109/jiot.2022.3186921.

[5] A. Al-Adhami, M. Ambroze, I. Stengel, and M. Tomlinson, “An Efficient Improvement of RFID Authentication Protocol Using Hash Function ZKP.”

[6] C. V. V. Aditya and R. K. Megalingam, “Zero-Knowledge Proof Based Authentication Over Untrusted Networks,” *Regular*, vol. 9, no. 9, pp. 238–241, Jul. 2020, doi: https://doi.org/10.35940/ijitee.i6917.079920.

[7] Wided Boubakri, Abdallah, W., & Noureddine Boudriga. (2017). *Access control in 5G communication networks using simple PKI certificates*. https://doi.org/10.1109/iwcmc.2017.7986606

[8] G. Venkatesh, S. V. Gopal, M. Meduri and C. Sindhu, "Application of session login and one time password in fund transfer system using RSA algorithm," 2017 International conference of Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, 2017, pp. 732-738, doi: 10.1109/ICECA.2017.8212763. keywords:

{Authentication;Protocols;Postal services;Personnel;Encryption;RSA Tokens;Random password number Generator;Session login},

[9] P. Soni, A. K. Pal and K. Khushboo, "A User Convenient Secure Authentication Scheme for Accessing e-Governance Services," 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kanpur, India, 2019, pp. 1-7, doi: 10.1109/ICCCNT45670.2019.8944393. keywords: {Authentication;Government;Password;Servers;Portals;Registers;e-Governance;Multi-server Authentication;RSA Cryptosystem;Two-factor Authentication},

[10] V. Mainanwal, M. Gupta and S. K. Upadhayay, "Zero Knowledge Protocol with RSA Cryptography Algorithm for Authentication in Web Browser Login System (Z-RSA)," 2015 Fifth International Conference on Communication Systems and Network Technologies, Gwalior, India, 2015, pp. 776-780, doi: 10.1109/CSNT.2015.90. keywords: {Authentication;Protocols;Cryptography;Servers;Databases;Computer hacking;ASP;SQL;Z-RSA;ZKP;MD5;RSA},

FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

Trimester, Year: Trimester 3, Year 3	**Study week no.: 2**
Student Name & ID: Ang Yong Seng 2002293	
Supervisor: Ts. Dr. Gan Ming Lee	
Project Title: Zero Knowledge Protocol Network Authentication and Monitoring	

1. WORK DONE

The work done are revising again the FYP1 report, so that I could catch back the progress. Due to the broad scope of project, I have started to search the information and would like to get a better view in how to implement the system. For instance, going to Squid proxy official documentation.

2. WORK TO BE DONE

The work to be done included finding the potential RSA libraries to be used, and the basic authentication method and study how it is being implemented.

3. PROBLEMS ENCOUNTERED

Realizing the research gap is still huge for me, I could only continue to fill in the gap by studying relevant material on the field.

4. SELF EVALUATION OF THE PROGRESS

It is required to be patient and dive into the information found via online resources, so that the research gap could be minimized.

GML

Supervisor's signature

Student's signature

FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

Trimester, Year: Trimester 3, Year 3	**Study week no.: 4**
Student Name & ID: Ang Yong Seng 2002293	
Supervisor: Ts. Dr. Gan Ming Lee	
Project Title: Zero Knowledge Protocol Network Authentication and Monitoring	

1. WORK DONE

I have finalized the RSA libraries, which is NodeRSA to be used in Node.js development for captive portal. However, the official documentation of Squid proxy is limited for me to get the idea of implementation.

2. WORK TO BE DONE

The next two weeks should focus on developing the captive portal in advance using the selected RSA libraries. Besides, I should try to find another source to learn how Squid could be implemented.

3. PROBLEMS ENCOUNTERED

Due to the uncertainty regarding project requirement, I have moved forward to study the coding of RSA. The example given in the Squid official website is lack of guidance in configuration.

4. SELF EVALUATION OF THE PROGRESS

It is kind of wasting time to study the coding of RSA libraries without any work done. Hence, I will start the development starting next two weeks.

GML

Supervisor's signature

Student's signature

FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

Trimester, Year: Trimester 3, Year 3	**Study week no.: 6**
Student Name & ID: Ang Yong Seng 2002293	
Supervisor: Ts. Dr. Gan Ming Lee	
Project Title: Zero Knowledge Protocol Network Authentication and Monitoring	

1. WORK DONE

The simple authentication has been implemented using the NodeRSA library via Visual Studio Code. Another website for deepening the understanding towards Squid has been found, which is webhostinggeeks.com.

2. WORK TO BE DONE

Before developing a captive portal, some assumption must be made such as how their human resources being accessed, creating some imaginary users for testing purpose in ZKP authentication. Next, performing the basic authentication using Squid proxy to familiarize the configuration in the Squid configuration file from the aspects of network authentication.

3. PROBLEMS ENCOUNTERED

The development of captive portal does not face significant problem. However, it is noticed that NodeRSA could only be used in server side. Hence, another library is required to find so that the signing operation could be implemented on client side without providing private key to the server.

4. SELF EVALUATION OF THE PROGRESS

The library should be investigated clearly before applying in the project. Else, it is time consuming to keep changing the library.

GML

Supervisor's signature

Student's signature

FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

Trimester, Year: Trimester 3, Year 3	**Study week no.: 8**
Student Name & ID: Ang Yong Seng 2002293	
Supervisor: Ts. Dr. Gan Ming Lee	
Project Title: Zero Knowledge Protocol Network Authentication and Monitoring	

1. WORK DONE

Another library which is WebCryptoAPI has been selected as library to implement signing operation in client side. After the testing, the authentication can be successful using WebCryptoAPI on client side and NodeRSA on server side with URL localhost:3000. Furthermore, basic authentication using Squid can be configured successfully.

2. WORK TO BE DONE

The registration page should be added so that the user could register themselves.
Trial of integration between the captive portal and Squid proxy should be done.

3. PROBLEMS ENCOUNTERED

It is found that the Squid proxy is commonly support the Python customized helper script, but not Node.js. Hence, I might need to consult project supervisor to find out the next step.

4. SELF EVALUATION OF THE PROGRESS

Currently, the progress is not satisfied because the network authentication part is still halfway only.

GML

Supervisor's signature

Student's signature

FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

Trimester, Year: Trimester 3, Year 3	**Study week no.: 10**
Student Name & ID: Ang Yong Seng 2002293	
Supervisor: Ts. Dr. Gan Ming Lee	
Project Title: Zero Knowledge Protocol Network Authentication and Monitoring	

1. WORK DONE

Registration page has been added and the user can register themselves.

I have discussed with project supervisor, and it is found that it is weird to have two server which are Squid proxy server and captive portal web server. Hence, he would like me to setup a proxy server which will redirect to captive portal by developing everything in either Squid proxy or Node.js. Due to consideration that we can have better flexibility to manage the key, I have chosen Node.js platform to continue the development.

Other than that, the scope of network monitoring has been minimized, which becomes a very small part in the project.

2. WORK TO BE DONE

Developing proxy server using Node.js library.
Starting to install Zabbix server and agent so that the resource usage could be monitored.

3. PROBLEMS ENCOUNTERED

It is found that some of the proxy server libraries using Javascript has no longer maintained and lack of documentation.

4. SELF EVALUATION OF THE PROGRESS

Focusing on the network authentication for two more weeks, and try to build a proxy server using the existing documentation.

GML

Supervisor's signature

Student's signature

FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

Trimester, Year: Trimester 3, Year 3	**Study week no.: 12**
Student Name & ID: Ang Yong Seng 2002293	
Supervisor: Ts. Dr. Gan Ming Lee	
Project Title: Zero Knowledge Protocol Network Authentication and Monitoring	

1. WORK DONE

I could only build an HTTP proxy server, but not HTTPS server.
Zabbix server and agent installation has been done.

2. WORK TO BE DONE

Implementation of testing and completing the report.

3. PROBLEMS ENCOUNTERED

Some bugs have been found during the testing, such as WebCryptoAPI could only be called in secure environment such as HTTPS, but our local development is only HTTP. Hence, I have changed the library again to jsrsasign.

4. SELF EVALUATION OF THE PROGRESS

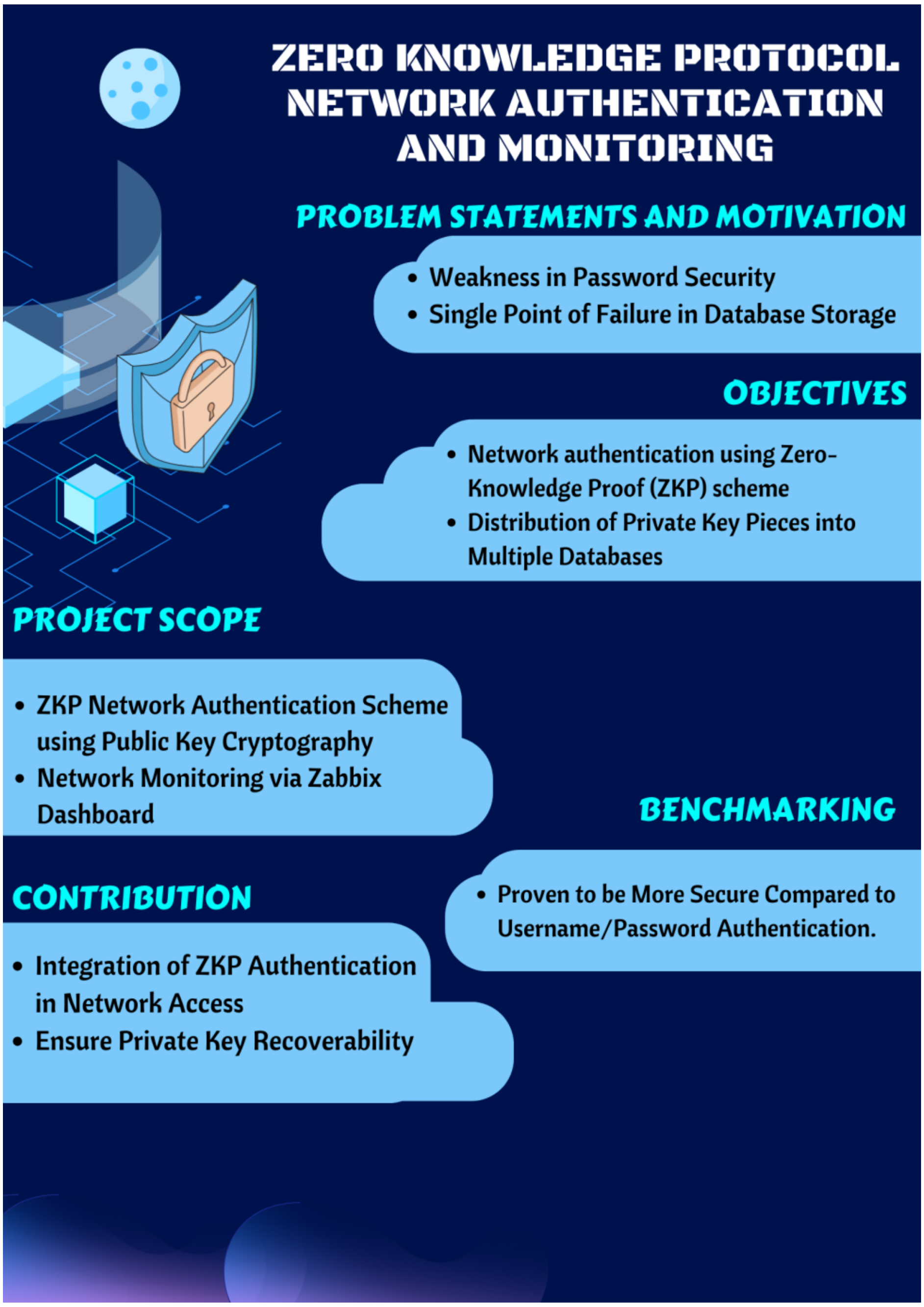
The report submission is a bit rush, but I will try my best to complete it.

GML

Supervisor's signature

Student's signature

POSTER



ZERO KNOWLEDGE PROTOCOL NETWORK AUTHENTICATION AND MONITORING

PROBLEM STATEMENTS AND MOTIVATION

- Weakness in Password Security
- Single Point of Failure in Database Storage

OBJECTIVES

- Network authentication using Zero-Knowledge Proof (ZKP) scheme
- Distribution of Private Key Pieces into Multiple Databases

PROJECT SCOPE

- ZKP Network Authentication Scheme using Public Key Cryptography
- Network Monitoring via Zabbix Dashboard

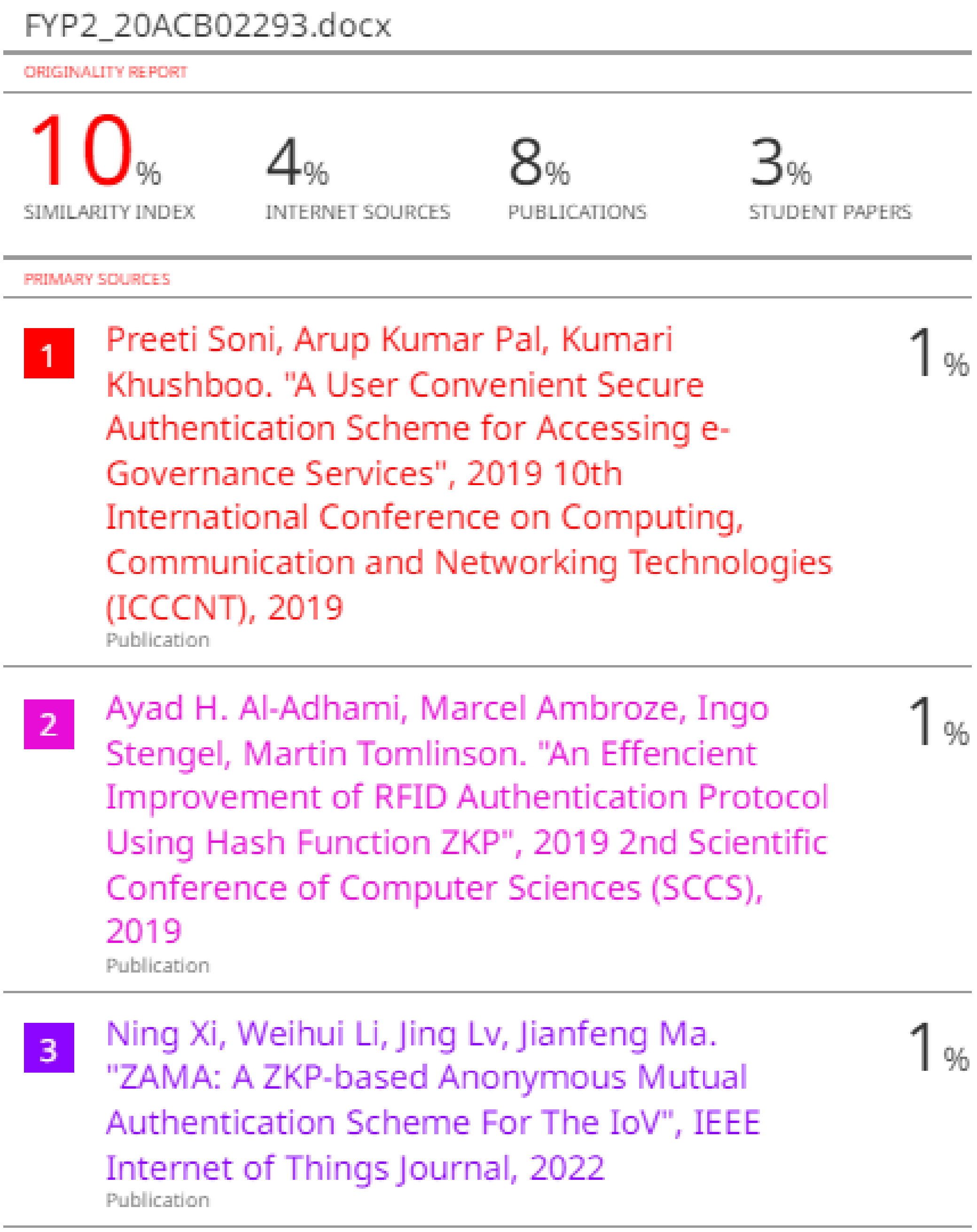
BENCHMARKING

- Proven to be More Secure Compared to Username/Password Authentication.

CONTRIBUTION

- Integration of ZKP Authentication in Network Access
- Ensure Private Key Recoverability

PLAGIARISM CHECK RESULT



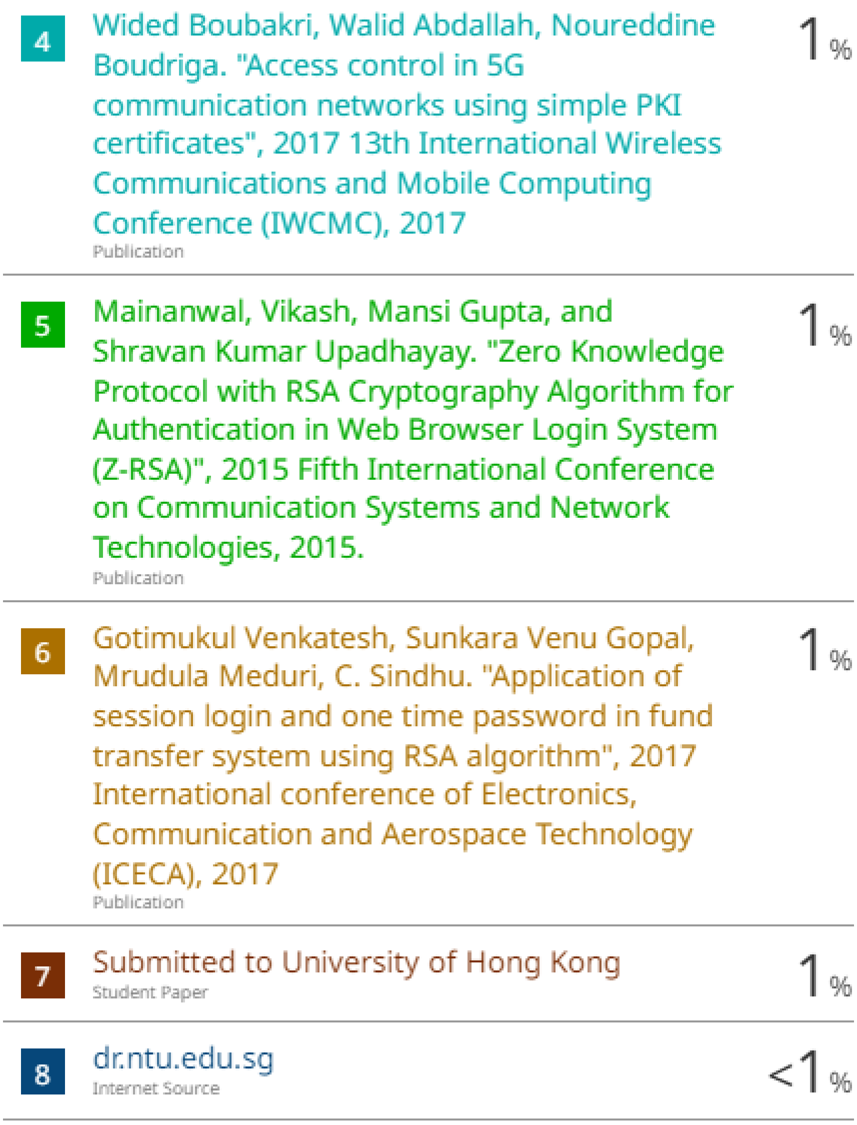
FYP2_20ACB02293.docx

ORIGINALITY REPORT

10%	4%	8%	3%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Preeti Soni, Arup Kumar Pal, Kumari Khushboo. "A User Convenient Secure Authentication Scheme for Accessing e-Governance Services", 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2019 Publication	1%
2	Ayad H. Al-Adhami, Marcel Ambroze, Ingo Stengel, Martin Tomlinson. "An Effencient Improvement of RFID Authentication Protocol Using Hash Function ZKP", 2019 2nd Scientific Conference of Computer Sciences (SCCS), 2019 Publication	1%
3	Ning Xi, Weihui Li, Jing Lv, Jianfeng Ma. "ZAMA: A ZKP-based Anonymous Mutual Authentication Scheme For The IoV", IEEE Internet of Things Journal, 2022 Publication	1%



4	Wided Boubakri, Walid Abdallah, Noureddine Boudriga. "Access control in 5G communication networks using simple PKI certificates", 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), 2017 Publication	1 %
5	Mainanwal, Vikash, Mansi Gupta, and Shravan Kumar Upadhayay. "Zero Knowledge Protocol with RSA Cryptography Algorithm for Authentication in Web Browser Login System (Z-RSA)", 2015 Fifth International Conference on Communication Systems and Network Technologies, 2015. Publication	1 %
6	Gotimukul Venkatesh, Sunkara Venu Gopal, Mrudula Meduri, C. Sindhu. "Application of session login and one time password in fund transfer system using RSA algorithm", 2017 International conference of Electronics, Communication and Aerospace Technology (ICECA), 2017 Publication	1 %
7	Submitted to University of Hong Kong Student Paper	1 %
8	dr.ntu.edu.sg Internet Source	<1 %

Universiti Tunku Abdul Rahman			
Form Title : Supervisor's Comments on Originality Report Generated by Turnitin for Submission of Final Year Project Report (for Undergraduate Programmes)			
Form Number: FM-IAD-005	Rev No.: 0	Effective Date: 01/10/2013	Page No.: 1of 1

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY

Full Name(s) of Candidate(s)	Ang Yong Seng
ID Number(s)	20ACB02293
Programme / Course	CN
Title of Final Year Project	Zero Knowledge Protocol Network Authentication and Monitoring

Similarity	**Supervisor's Comments** **(Compulsory if parameters of originality exceeds the limits approved by UTAR)**
Overall similarity index:___10_____ % **Similarity by source** Internet Sources: __4____________% Publications: ___8 ___________ % Student Papers: ___3___________ %	
Number of individual sources listed of more than 3% similarity: _0________	
Parameters of originality required and limits approved by UTAR are as Follows: **(i) Overall similarity index is 20% and below, and** **(ii) Matching of individual sources listed must be less than 3% each, and** **(iii) Matching texts in continuous block must not exceed 8 words** ***Note: Parameters (i) – (ii) shall exclude quotes, bibliography and text matches which are less than 8 words.***	

Note Supervisor/Candidate(s) is/are required to provide softcopy of full set of the originality report to Faculty/Institute

Based on the above results, I hereby declare that I am satisfied with the originality of the Final Year Project Report submitted by my student(s) as named above.

GML

______________________________ ______________________________

Signature of Supervisor Signature of Co-Supervisor

Name: __Gan Ming Lee _____ Name: __________________________

Date: __26/04/2024__________ Date: ____________________________

UNIVERSITI TUNKU ABDUL RAHMAN

FACULTY OF INFORMATION & COMMUNICATION TECHNOLOGY (KAMPAR CAMPUS)

CHECKLIST FOR FYP2 THESIS SUBMISSION

Student Id	20ACB02293
Student Name	Ang Yong Seng
Supervisor Name	Ts. Dr. Gan Ming Lee

TICK (√)	**DOCUMENT ITEMS** Your report must include all the items below. Put a tick on the left column after you have checked your report with respect to the corresponding item.
√	Title Page
√	Signed Report Status Declaration Form
√	Signed FYP Thesis Submission Form
√	Signed form of the Declaration of Originality
√	Acknowledgement
√	Abstract
√	Table of Contents
√	List of Figures (if applicable)
√	List of Tables (if applicable)
	List of Symbols (if applicable)
√	List of Abbreviations (if applicable)
√	Chapters / Content
√	Bibliography (or References)
√	All references in bibliography are cited in the thesis, especially in the chapter of literature review
	Appendices (if applicable)
√	Weekly Log
√	Poster
√	Signed Turnitin Report (Plagiarism Check Result - Form Number: FM-IAD-005)
√	I agree 5 marks will be deducted due to incorrect format, declare wrongly the ticked of these items, and/or any dispute happening for these items in this report.

*Include this form (checklist) in the thesis (Bind together as the last page)

I, the author, have checked and confirmed all the items listed in the table are included in my report.

____

(Signature of Student)
Date: 25/04/2024