CHAPTER I

INTRODUCTION

Project Context

In today's digital landscape, secured messaging applications have become increasingly important due to the growing demand for privacy and security. With the rise of digital communication in personal, business, and governmental domains, ensuring the security of sensitive information against unauthorized access and cyber threats has become of utmost importance.

One of the main methods to protect information security is the use of cryptography techniques. Along with keeping the information private, it also performs other tasks like system security, digital signature, authentication, and secret sub-storage. In order to prevent information from being altered, forged, or counterfeited, the encryption and decryption solution can guarantee the confidentiality of the information as well as its integrity and certainty. Encryption techniques, specifically the Rivest Shamir Adleman (RSA) and Advanced Encryption Standard (AES) algorithms, offer an appealing solution for protecting data.

To meet the rising demand for secure communication, Safe-on-Chat is a messaging application that aims to offer privacy and security features. The resulting application will give users an effective and clever way to communicate securely across various applications, where data security is an essential component. The study's main goal is to develop a messaging system that can effectively deal with the growing risks of unauthorized access and data breaches. The application strives to provide data security

by incorporating both RSA and AES encryption algorithms. By offering reliable communication solutions across various domains, the research's findings could advance the field of secured messaging.

Purpose and Description

Purpose of the Study

The purpose of this study was to develop and implement a messaging application for widespread usage that will not compromise the privacy and security features through the use of RSA and AES encryption algorithms with the aim of ensuring the confidentiality and integrity of shared data where information security is critical.

Description of the Study

Safe-on-Chat is a proposed messaging application that aims to provide users with overall data protection by integrating RSA and AES encryption algorithms, utilizing technologies and frameworks, and performing testing to confirm the application's integrity, reliability, and usability. The goal of this study was to significantly advance the field of free for commercial use secure messaging applications by employing RSA and AES encryption algorithms.

Objectives of the Study

Main Objective

The main objective of this thesis was to develop and implement a messaging application that employs the RSA and AES encryption algorithms to provide the confidentiality and integrity of shared data as well as to create a user-friendly interface

that is simple and easy to use. This thesis extended the goal of creating a free messaging system that works with different devices and operating systems.

Specific Objectives

Specifically, the researchers defined objectives to achieve their study's aims, guiding their investigations and contributing to the overall goal. These goals helped them focus their attention on what was crucial and addressed the important components of the study.

The specific objectives are as follows:

1. To offer data security and confidentiality in communication by implementing the RSA and AES encryption algorithm.
2. To provide security measures against internet threats and unauthorized access for secure communication.
3. To design and create a user-friendly interface that is simple to navigate that users of the application have a smooth and easy-to-use experience.
4. To offer user authentication mechanisms to verify the identities of message senders and receivers, preventing impersonation and unauthorized access.
5. To evaluate the following performance of the system in terms of ISO 25010. Through survey questionnaires as well as compiling suggestions and recommendations, forming a basis for improvements in future system development.

5.1 Functionality,

5.2 Usability,

5.3 Efficiency,

5.4 Security,

5.5 Compatibility,

5.6 Maintainability,

5.7 Portability, and

5.8 Efficiency

Conceptual Paradigm

In this section, the researchers outline the conceptual framework of the system. A conceptual framework is a structure that lists the main ideas, factors, connections, and expectations which guide academic studies. It offers a theoretical framework as well as a perspective for analyzing data. To comprehend research issues, it makes use of pre-existing ideas, models, or expertise. It provides all of the objectives of the study, identifies variables, formulates research questions, and leads the choice of methods and data analysis strategies. Conceptual frameworks can be mathematical, taxonomic, or literary.

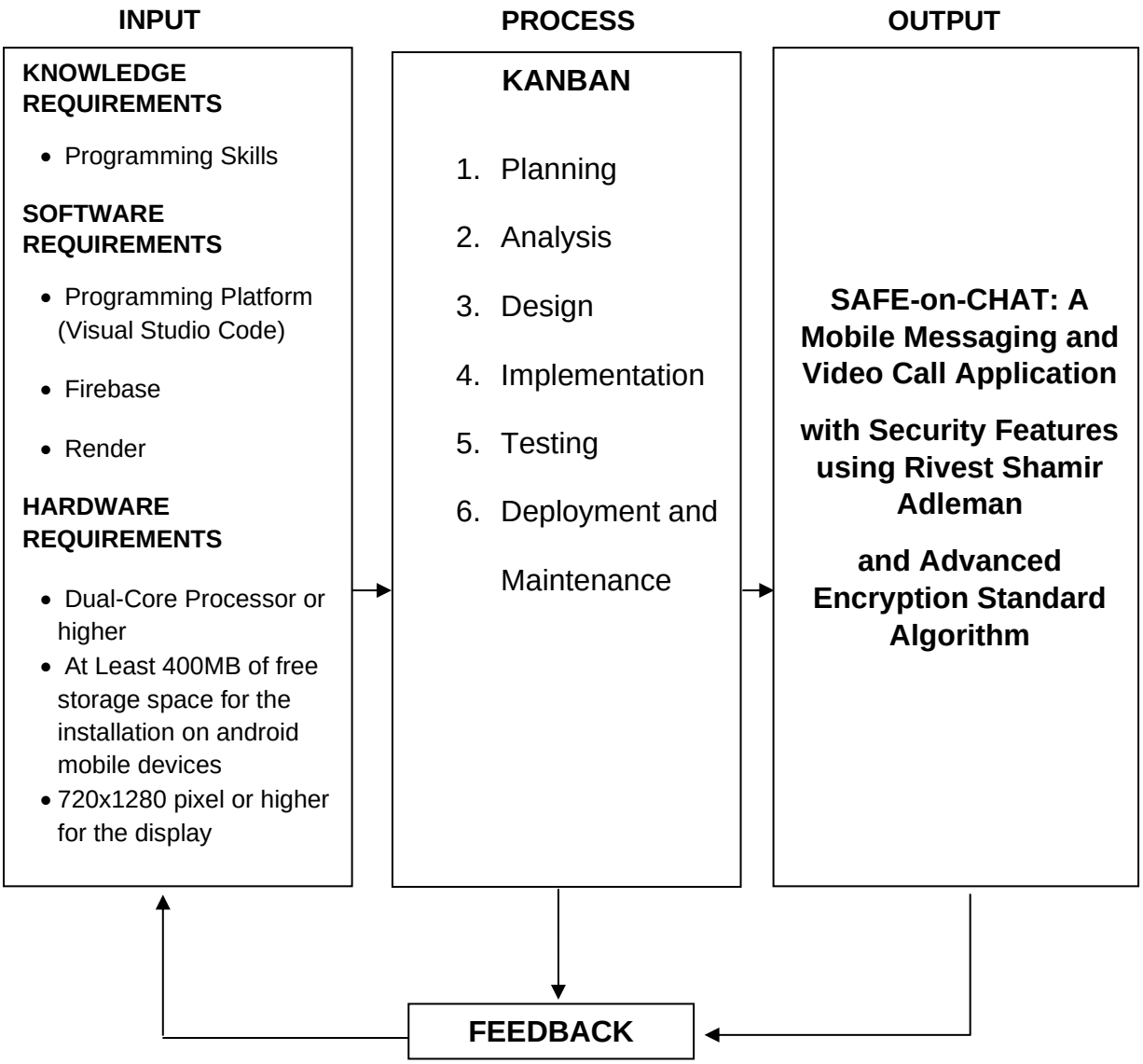

Figure 1. Conceptual Paradigm

The figure 1 above shows the conceptual paradigm. It describes the theoretical foundation and framework on which a study is built. It establishes the concepts, variables, relationships, and assumptions that form the basis of the research design. The figure above depicts the process and particular kanban method employed in this study, as well as the software and hardware requirements for the system that must be built.

Scope and Limitations

The scope of the study focused on creating a messaging application using RSA and AES encryption algorithms. It involves designing and implementing these algorithms for encryption and decryption, as well as incorporating a user-friendly interface and log-in options using both PIN and fingerprint, offering a more protected and private communication experience. The application can send files, videos, images, and text messages; create group chats; and make video and audio calls. The application also has an online indicator and pop-up notifications. Furthermore, the application disables screenshots inside the chat rooms.

The proposed messaging application also comes with some limitations. Only tablets and mobile phones can access it. Any other devices like desktops, laptops, smartwatches, and smart TVs cannot access the system. The application cannot customize the chat app's interface and cannot limit the number of users who want to access it.

Significance of the Study

The significance of creating a new messaging application using AES and RSA encryption algorithms lies in its potential to address a critical challenge in modern communication technology: security.

The use of the AES and RSA encryption algorithms provides the messaging application with reliable security. Given the increasing number of cyber-security threats and data breaches, using an encryption technique known for its strength and reliability

can offer users the trust that their messages are secure from interception and unauthorized access.

Therefore, the implementation of a messaging application with an encryption algorithm has the potential to improve communication security. Upon deploying this proposed system, there will be beneficiaries when using this proposed messaging application, which are the end users and the future researchers to use this study as their reference.

The **End Users** would be able to use a messaging application that offers data security.

And **future researchers** can use the study for providing insights about secured communication systems and privacy protection that can be relevant based on the results and findings of this study for their future references.

Definition of Terms

Advanced Encryption Standard (AES) Encryption Algorithm

is a highly trusted encryption algorithm used to secure data by converting it into an unreadable format without the proper key.

Communication defenses

are measures or strategies implemented to protect communication systems and networks from unauthorized access, data breaches, or other security threats.

Cyber attacks

are deliberate and malicious activities or attempts to compromise, disrupt, or gain unauthorized access to computer systems, networks, or digital infrastructure.

Cyber threats

are potential risks and dangers that target computer systems, networks, or digital infrastructure, including malicious activities like hacking, malware, phishing, and other cyber-attacks.

Data breaches

are incidents where unauthorized individuals gain access to sensitive or confidential data, potentially leading to data theft, loss, or misuse.

Encryption techniques

are methods used to convert plaintext into ciphertext to protect data confidentiality and integrity.

Hackers

are individuals with advanced knowledge and skills in computer systems and networks who seek to gain unauthorized access, exploit vulnerabilities, or disrupt operations for various purposes.

Rivest Shamir Adleman (RSA) Encryption Algorithm

is an asymmetric cryptography that employs both a public key and a private key. A public key is distributed publicly, as its name implies, whereas a private key is kept private and must never be disclosed.

Security assurance

includes measures, practices, and processes that ensure the confidentiality, integrity, availability, and reliability of systems, data, and information, providing confidence in their protection against unauthorized access or harm.

Symmetric key block cipher

is a type of encryption algorithm that uses a single key for both encryption and decryption. It operates on fixed-size blocks of data and transforms them into ciphertext.

Unauthorized access

is gaining access to data, systems, or networks without proper authorization or permission. It is a security breach and a significant concern in terms of data protection.