CHAPTER 1

INTRODUCTION

1.1 Introduction

The technological advancement of smartphones has proved to be a magnificent journey that has altered the way we interact with one another, conduct business, and access information. There are a lot of key turning points in the development of smartphones. From restricted use for calls and messages in the 1990s, phones evolved to advanced features such as basic web browsing and emails experienced by a user who has BlackBerry. When the iPhone was introduced around 2007, the phone industry bloomed with the touchscreen feature and came along with Android in the market (Wahlström et al., 2016). Now, smartphones can be connected to the internet and users can experience having a 'mini-computer' by their palms. The rapid evolution of highly convenient smartphones has significantly reduced the time and effort required to complete daily tasks.

Today, smartphones have integrated into humans' lives that allow humans to connect to anything such as information, education, finances, and healthcare. A lot of applications in smartphones cater to humans' daily activities such as text messages, internet browsers, social media, and many more (Buja, 2018). These activities certainly benefit people in many ways, but with the vast amount of data being transmitted across the network of mobile phones, it is now crucial to protect that data especially data related to personal, financial, health, and work information. These details, including ones about money, health, social activities, and other matters, might

be easily jeopardized and result in unauthorized access to this crucial information (Li et al., 2018). If this information falls into the wrong hands, it may lead to identity theft where the criminal can use the user's identity to open new accounts that can bring lots of harm to the user, or financial fraud, where the unauthorized person can have access to user's bank account and steals the money. In addition to the risks mentioned above, a data breach can also have a negative impact on the user's reputation and can result in legal repercussions.

1.2 Problem Background

Numerous industries have benefited from the evolution of smartphones by incorporating them into their daily operations, which has helped those industries expand. Smartphones are not just used by people to access data; large industries like healthcare, education, and even technology businesses use them to their advantage. This allows them to participate in society and remain competitive in their respective fields. Various developments demonstrate how much smartphones are influencing various industries. From manually written down documentation to online fill-out forms and from getting cash at the counter to online banking, these evolutions show how much smartphones influence these sectors.

Due to smartphones' enormous popularity, privacy and security concerns are now indispensable. Due to their size, smartphones are highly probable to be misplaced, stolen, or readily obtainable to those without authorization. Smartphones are substantially more inclined to theft than desktops because once an intruder has physical access to a device, he or she may be able to pose as the primary proprietor of the device for monetary or non-monetary benefits and mischief (Al-Rahman et al., 2018).

Previously, a lot of sensitive data was stored on hard discs and printed versions where this information is stored in secure places and only authorized persons can access these secured places. However, with the widespread use of smartphones, it has become nearly difficult to prevent or inhibit an individual or organization from utilizing smartphones as a tool to store data. Designing ways to secure information access via smartphones is the only way to prevent the damage from escalating more severely (Bahaddad et al., 2022).

With a large amount of data accessible through smartphones, such as private documents kept in a locked room away from intruders, this data must be fully secured and safeguarded to prevent sensitive data exposure that could result in a number of bad difficulties for the users. To protect people's safety and the security of their data, information security is crucial. Smartphone information security is a crucial component of protecting private data and maintaining the integrity and privacy of mobile devices. Knowing about and executing information security measures into practice is crucial to protect against potential threats and vulnerabilities given the growing reliance on smartphones for a variety of activities, including communication, banking, social media, and online shopping (Karimi & Krit., 2019). Examples of the most common information security in smartphones are password and biometric authentication or even advanced, Two-Factor Authentication (2FA). These examples implement cryptography.

Cryptography is a crucial part of information security technology because it safeguards communications and transactions as well as personally identifiable information (PII) and other sensitive data. Digital signatures are a subfield of cryptography that strengthens confidentiality, integrity, and authentication for digital interaction. Confidentiality, integrity, authentication, and non-repudiation are four key

information security goals a Digital Certificate can aid with. Confidentiality ensures that information can only be accessed by authorized parties, while integrity checks to see if the data has been compromised. Non-repudiation prevents someone from denying they transmitted or received the data, while authentication ensures that one can establish their identity (Karimi & Krit, 2019).

There are several applications for cryptography on mobile devices. Since most smartphones have built-in encryption technology that regularly protects the data stored on them, device encryption is one of the most well-known and user-friendly forms of encryption. Even if someone manages to physically touch the device, they won't be able to access the data without the encryption key or passcode. Biometric security is another well-known and frequently applied cryptography in smartphones (Im et al., 2020). To prevent fraudsters from accessing the device and to safeguard users' privacy, biometrics like fingerprint sensors and face recognition are encrypted. Mobile devices also apply Secure Authentication techniques where this cryptographic technique is used to confirm the identities of users while conducting secure authentication. Secure connections between smartphones and authentication servers are frequently set up using public-key cryptography, like the Rivest–Shamir–Adleman (RSA) methods, to make sure that only approved individuals may access certain products or applications (Baqeel & Saeed, 2019).

The majority of cryptographic protocol suites include digital signatures as a basic component. They are frequently used for software distribution, financial transactions, contract oversight applications, and other circumstances in which it is crucial to identify fraudulent activity or alteration. Digital signatures can be established and authenticated on smartphones using cryptographic methods. With the aid of digital

signatures, it is possible to confirm the veracity and authenticity of digital documents or transactions and ensure that they were not altered during transmission.

1.3 Problem Statement

Awareness of information security has had a favorable influence on the market's expanding development of security products in a variety of industries. The majority of individuals utilize their smartphones for various activities, including communication, internet browsing, email correspondence, professional tasks, and educational pursuits. It is estimated by the end of 2025, out of the 8 billion people on the planet, there will be 7.49 billion mobile users globally (O'Dea, 2021). Data tapping and alteration may culminate in loss of availability, integrity, and confidentiality, as well as other possible losses like loss of life, money, and assets (Phun et al., 2021). For the foregoing reason, information security is paramount. To protect the security of user data on smartphones, encryption is an essential aspect of security products. An attempt to increase the security of the information in smartphones starts with applying cryptography in applications used in smartphones especially applications that require storing and accessing important data. With the help of the assistive application of cryptography, smartphones that contain applications that store information can increase, improve, and maintain the credibility, integrity, and availability of the data stored (Phun et al., 2021). It is a common security application in email messages, online banking apps, and clouds that stores files and folders replacing the hard disc and physical documentation. All these applications require users to input their user names and passwords to allow access to their information. Users will feel more satisfaction in using the applications if security

implementations are embedded in these applications in smartphones. Figure 1.1 shows the flow of simple authentication in applications.

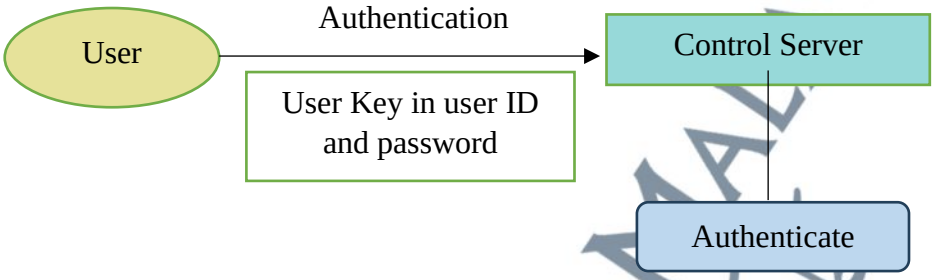

Figure 1. 1: Simple Authentication in Smartphone Application

Having a user input their user's name and password is one of the basic security applications since the majority of applications in smartphones use this security tool. If developed and maintained poorly, simple verification processes like entering a username and password might constitute security dangers. Here are some potential privacy flaws that using simple authentication techniques may cause (Nimmy et al., 2021). A common type of cyberattack while using a simple verification process is credential theft, in which attackers use a variety of methods, such as phishing, keylogging, and data breaches, to illicitly obtain usernames and passwords. Once acquired, these credentials can be used to log into the application and perhaps take over access to the user's private data.

Besides, Man-in-the-Middle (MIM) attacks can also happen where without adequate security measures, an attacker can eavesdrop on, alter, or pretend to be a user during their login session by taking over the data exchange between the smartphone application and the server (Henricks & Kettani, 2019).

Another famous security attack is known as Brute-force attack where attackers have a means to get unauthorized entry to the software by using computerized methods to recurrently guess passwords. Passwords that are weak or predictable can be decrypted fairly swiftly.

With all the downsides of simple authentications have been discovered, an advanced way to increase the authentication of smartphone applications has been implemented. By requiring a pair of different kinds of authentication factors to validate a user's identity, two-factor authentication (2FA) on smartphones offers an additional degree of security to your accounts (Henricks & Kettani, 2019). As its name, 2FA functions by having two authentications where the primary authentications enable the user to log in to their account using their user's name and password. Once the user managed to log in, they were still not able to access the applications without bypassing the second authentication. Here, to pass the second authentication, users need to key in things that they have. The most common method used in second authentication are One-time Password (OTP) via Short Message Services (SMS) where the user will receive a unique code via text message in a registered number that requires the user to key in the number in the application for them to be able to access the application (Anusas-Amornkul, 2019). When the application receives accurate input for both the primary and secondary authentication elements, it will authenticate the user's identity and enable the user to access to user's account. By employing two factors, this can ensure that even if intruders were to discover or guess a legitimate user's password, they would still need to have access to the user's smartphone or the secondary authentication mechanism to enter the application. This increases security and makes it much more difficult for unauthorized individuals to access your accounts (Tirfe & Anand, 2022). Figure 1.2 shows the flow of 2FA.

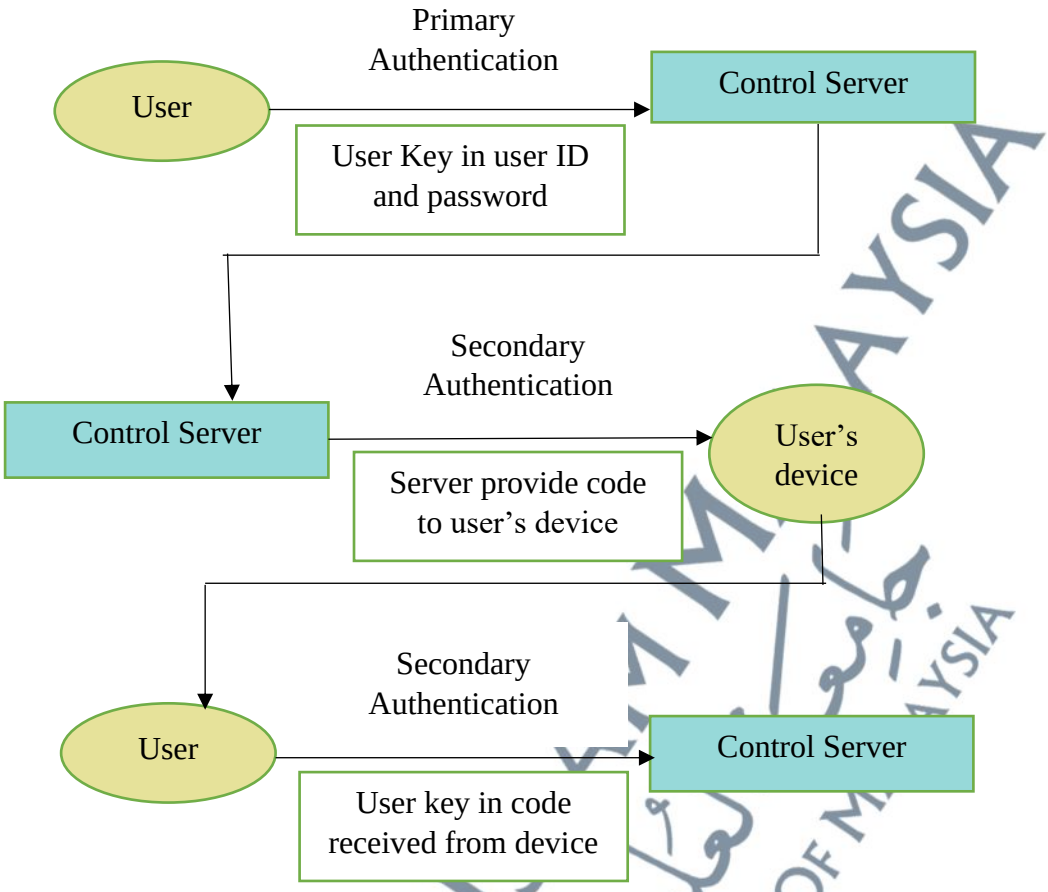

Figure 1. 2: Flow of 2-Factor Authentication

Even though 2FA adds a layer of safeguarding, it is not impervious to all potential security risks. Here are a few potential threats connected to 2FA such as SIM swapping where attackers may attempt to carry out a SIM swapping attack in situations when SMS-based 2FA is employed. They make contact with the user's cell service provider while posing as the account owner and demand a substitute SIM card (Kulah *et al.*, 2019). The SMS with the authentication code can be retrieved and the 2FA method can be avoided by acquiring ownership of the victim's phone number. Device theft: If the device utilized as the second factor of authentication is lost or taken, an intruder may be able to gain entry to the authentication codes on the device or bypass

the second factor if the device lacks sufficient security features, like a PIN or biometric authentication. Besides, the second authentication in a smartphone application that requires a Transaction Authorization Code (TAC) can also be jeopardized by TAC fraud (Oh *et al.*, 2019). Where cybercriminals exploit legal TACs to execute unauthorized monetary activities or illicit transactions. To fool people into giving their TACs, fraudsters may use phishing techniques. They might produce phony websites that look like official banking or financial institutions, send phony emails or SMS messages, or do all three. It's possible to trick unsuspecting victims into giving up their TACs, enabling the fraudsters to carry out unauthorized transactions (Nwabuwe *et al.*, 2023).

Besides the issue of vulnerabilities in authentication for smartphone applications, the conservative encryption in the market requires high power consumption and huge memory in a device. Although nowadays smartphones have produced more powerful processors and increased memory capacity it is still limited compared to desktops, thus, less practical for conservative encryption to be implemented in smartphone applications (Salunke et al., 2019). With all the problems explained the suggested solutions are explained in section 1.4 below.

1.4 Motivation

One of the reliable authentication methods using cryptography is applying digital signatures. Utilizing cryptographic methods, authentication with a digital signature includes confirming the authenticity and integrity of a digital message or document. It offers confirmation that the message or document was transmitted by the alleged sender and was not altered. To utilize digital signature as authentication in smartphone applications, both the user and the device which is the user's smartphone

must be available at the same time for the authentication to work. The digital signature requires the server to create a public key and private key for both the user and the device respectively. This can be implemented using the Rivest-Shamir-Adleman (RSA) algorithm since RSA requires to production of two keys, which are the public key and private key.

Authentication using a digital signature also requires a third-party trustee known as a Certificate Authority (CA). CA is responsible for binding the public key of the user and the device to their respective owner to ensure that the key is reliable from the genuine owner. CA then produced a Digital Certificate for the user and device. This certificate contains a digital signature that is used for authentication in a smartphone application is one way to secure data in an application to ensure that the authentication is really from the user. Having a smartphone to be used as a device to authenticate together with the user can also reduce TAC fraud and phishing from intruders (Nwabuwe et al., 2023).

Besides authentication using digital certificates, lightweight authentication algorithms can be implemented in smartphone applications. The lightweight algorithm requires low consumption of memory and processor power, suitable for smartphones that have limited processor power and memory.

In conclusion, this research aims to develop authentication using a digital signature to authenticate both the user and the device in a smartphone application to increase the secure authentication of an application. The proposed authentication is designed as an authentication model for smartphone users.

1.5 Research Questions

Based on the identified research problems, six research questions are listed in Table 1.1 below:

Table 1. 1: List of Research Questions

No.	Research Question
1.	What is the current research trend in authentication method algorithms for smartphone users?
2.	What is the trend of attacks that jeopardize the authentication for smartphone applications?
3.	What are the security requirements and mechanisms needed to solve the authentication attacks in smartphone applications for users?
4.	Which cryptography algorithm is suitable to use to achieve authentication requirements in smartphone applications?
5.	How does the digital certificate used in the proposed model verify both the user and the device in smartphone users?
6.	Is the proposed authentication model applicable for authenticated users and devices for smartphone users?

1.6 Research Objectives

The main aim of this research is to propose a user-device authentication model with digital certificates for smartphone users. In achieving the main objective, the following Table 1.2 are the specified objectives of the research.

Table 1. 2: List of Research Objectives

No.	Research Objective
1.	To analyze authentication requirements for applications in smartphone users.
2.	To design an authentication model to authenticate user and device for application in smartphone user.
3.	To evaluate the user-device authentication model with digital certificate on the ability to verify both the user and device for smartphone application.

1.7 Research Scope

The research sought to examine the scope of the authentication in smartphone user. Table 1.3 below explains the research inclusion and exclusion criteria for the authentication model.

Table 1. 3: Research Inclusion and Exclusion Criteria

Scopes	Inclusion Criteria	Exclusion Criteria
Data Security	The authentication of the user and device must be the major element of the proposed model.	The element besides authentication of the user and device for the proposed model.
Element for authentication	The authentication for both the user and the device of the user.	The authentication besides both users and the device of the user.
Expert Evaluators	The experts to review must be lecturers and industrial individuals who have strong fundamentals in information security	Experts who have limited to no information security background.

Table 1.3 above explains the inclusion and exclusion criteria for the whole research. The research is done by designing the user-device authentication model with digital certificates for smartphone user. Data security contains four important elements which are protection, detection, verification, and reaction. The proposed model will focus on the authentication and verification of the application in smartphone user. Both the user and the device must be included in the verification process (Bahaddad et al., 2022). Without both, the proposed model will not successfully authenticate the user to access the application in smartphone. The proposed model will be evaluated by expert

reviews who have strong fundamentals in information security so that they can answer the questionnaires without bias and lack of knowledge in information security.

1.8 Research Contribution

This research is aimed at applying digital certificates for the verification process. The authentication includes the user and the device for stronger authentication and to avoid data breaches. This research can differentiate between verification using the user only and using both the user and the device. This can ensure that the authentication in smartphone applications can be enhanced for better security assurance of the information stored in smartphone. The proposed user-device authentication with digital certificate for smartphone user can be beneficial to academic and industry research in a variety of ways. Academically, the proposed User-Device Authentication Model can contribute to the advancement of academic research in the field of authentication. This can result in enhanced and effective authentication techniques, as well as an improved comprehension of security and privacy issues related to user-device authentication. For industry, the proposed authentication model between the user and the device contributes to the development of industry knowledge by offering new perspectives on the implementation and application of authentication techniques in the real world as well as providing opportunities for mobile developers to develop better authentication process in applications for better security features in their application. This can assist organizations in enhancing security and safeguarding their users' information.

1.9 Research Structure and Organization

The structure of this research is organized based on the researched questions and objectives. The proposed methods are used to achieve the objectives of this study. Table 1.4 shows the constructed research methodology that explains the specific method for research objectives and questions.

Table 1. 4: Research Structure and Proposed Methods

Research Questions	Research Objectives	Methods
a) What is the current research trend in authentication method algorithms for smartphone user?	1. To analyze authentication requirements for applications in smartphone user.	i) Define research areas, research problems, objectives and scope
b) What is the trend of attacks that jeopardize the authentication for smartphone applications?		ii) Review Literature on authentication requirements for smartphone user.
c) What are the security requirements and mechanisms needed to solve the authentication attacks in smartphone applications for user?	2. To design an authentication model to authenticate user and device for application in smartphone user.	iii) Identify the requirements and scope of the authentication model for smartphone user.
d) Which cryptography algorithm is suitable to use to achieve authentication requirements in smartphone applications?		iv) Proposed an authentication model based on user and device authentication implementing digital certificates for smartphone user.
e) How does the digital certificate used in the proposed model verify both the user and device in smartphone user?	3. To evaluate the user-device authentication model with digital certificate on the ability to verify both the user and device for	v) Questionnaires answered by expert reviews to validate the user-device authentication model.

f) Does the proposed authentication model applicable for authenticate user and device for smartphone user?	smartphone application.	vi) Calculate the outcome data using the mathematical formula used in the model.

Table 1.4 shows the methods used in each research question to reach the objective of the research. For the first and second research questions, the method used is to define the research areas, problems, and literature review from previous research. The second objective is completed by identifying the requirements of authentication and proposing the authentication model with digital certificates for smartphone user. The last objective is obtained by questionnaires answered by experts as well as mathematical calculations of the formula used in the proposed model to achieve the expected outcome.

Chapter 1 provides an overview of the methodology of the study that resulted in the issue statement and the research questions. Although the view of the relationship based on two user experience elements came first which are the user and the device of the user, the aims of the research were clearly stated to address the research questions. The entire first chapter displays the broad strokes of the entire study, outlining how the thesis and research were organized before providing a summary.

In Chapter 2, the main concepts of the research are gathered from the relevant literature reviews. The systematic review is used to identify the overall data security information, the authentications of the user and device, implementing digital certificate for authentication purposes as well as proposed authentication model for user and device implementing digital certificate for smartphone user.

Chapter 3 explains the methodology of the research as well as the outcome of each of the objectives.

Chapter 4 explains the user interface of the proposed model as well as the elements used in the model. Step-by-step of the authentication model is explained for better understanding.

Chapter 5 explains the data collected and the analysis of the data based on the questionnaires. This chapter also explains the expected outcome by calculating using the formula used in the model.

Chapter 6 explains the conclusion of overall of the overall research as well as the research limitations and further research.

1.10 Summary

The emergence of smartphones can be attributed to the fusion of advances in computer power, mobile communication technology, and customer demand for high-end functionality in a portable device. As cellphones continue to play a significant part in our lives, it is essential to protect the data that is stored on them. To protect smartphone data, manufacturers, operating system providers, app developers, and users need to apply and adhere to best security practices.