CHAPTER 6

CONCLUSION AND FUTURE WORKS

6.1 Introduction

This chapter concludes and revises the research objectives and the outcome of the research. The research results show that the studies are effective in answering all the fundamental research questions, matching each study result to its research purpose to emphasize the importance of the whole research process. Furthermore, not only does this research provide an in-depth analysis of its value and implementation, but it also provides a brief overview of its limitations while providing valuable advice for future work.

6.2 Research Summary

Authentication in smartphone users is one of the many security requirements in current technologies especially when it comes to smartphones since the rapid growth of smartphone users. A lot of sensitive and private data must be secure from unauthorized access. Verifying authentication in smartphones is essential for a variety of reasons, as it has a direct impact on the device's overall security and privacy, as well as the user's data.

Smartphones contain a wide range of personal and confidential data, such as contact information, messages, photographs, financial information, and more, which must be authenticated to prevent unauthorized access, protect user privacy, and

reduce the risk of identity theft and data breaches. The fact that many individuals store their banking and payment credentials on their mobile devices for ease of use. Implementing robust authentication protocols helps safeguard these financial resources from theft or fraud.

This research outlines three primary research objectives to address the primary objective of the research. These objectives are: (1) To analyze authentication requirements for applications in smartphone user, (2) To design an authentication model to authenticate user and device for application in smartphone user, and (3) To evaluate the user-device authentication model with a digital certificate on the ability to verify both the user and device for smartphone application.

6.2.1 Research Objective One

The research objective one is to analyze authentication requirements for applications in smartphone user. To achieve this objective, two methods have been carried out. The first is to define the research areas, research problems, objectives, and scope of the authentication in smartphone user. Besides, reviewing literature and research done by other researchers related to the authentication in smartphone user are also done.

6.2.1.1 Research Contribution One

Implementing cryptography components for authentication in smartphone user was analyzed from existing works that have been discussed in Chapter 2 of this research. From the asymmetric cryptography chosen, the RSA algorithm is decided to be used for

authentication. The outcome of the research method for research objective one is considered as Research Contribution 1. This contribution is used as an input for Research Objective 2.

6.2.2 Research Objective Two

Research Objective 2 is to design an authentication model to authenticate user and device for application in smartphone user. To achieve the research objective, identifying the requirements and scope of the authentication model for smartphone user is necessary to outline the proposed authentication model based on the user and the device authentication implementing digital certificate for smartphone user. The user and the device information are encrypted using public key and private key of respective users and device.

6.2.2.1 Research Contribution Two

One of the secure cryptographic components identified in research two is using RSA algorithm. The user and the device information are encrypted using public key and private key of respective users and device. The authentication and verification of the user and the device using Digital Signature as the algorithm. The information is also signed using the RSA algorithm for authentication process. The research contribution two is an authentication model to authenticate user and device with digital certificate for smartphone user.

6.2.3 Research Objective Three

The research objective three is to evaluate the user-device authentication model with digital certificate on the ability to verify both the user and the device for smartphone application.

6.2.3.1 Research Contribution Three

This research is conducted in a qualitative method. There are two ways to evaluate the authentication model proposed. The first evaluation is done using a questionnaire to be answered by expert reviews to validate the user-device authentication model. This is done by conducting a presentation session with the selected experts to explain the flows of the proposed model and allowing them to answer the questionnaire based on the proposed model. Besides having answered the questionnaire, the model is also evaluated based on the calculation of the outcome data using the mathematical formula used in the model. The expected verification results determine whether the user and device can be authenticated using the formula used in the authentication model.

6.3 Research Implications

The authentication model proposed for smartphone users has the potential to provide numerous expected advantages. The implementation of user and device authentication facilitates the implementation of 2FA, which provides an additional layer of protection by requiring a combination of something the user is familiar with (password) and something they possess (device). The proposed model encrypts the information from the user and the device using RSA Public Key and Private Key and

the encrypted data is signed using Digital Signature. The idea of authenticating the devices and users is essential for the successful execution of mobile banking and payment transactions. It facilitates the secure execution of financial transactions.

This proposed model requires the user to authenticate together with their smartphone. This can ensure that only the legitimate of the account can have access and even if the unauthorized individual manages to get information about the user, they still require the user's device to log in. The implementation of authentication for users and devices provides an additional layer of protection. It guarantees that only authorized individuals can gain access to a device and its information, thus decreasing the likelihood of unauthorized access and data theft.

6.4 Research Limitation

The limitations of this research are as follows:

1) To streamline the user-device authentication process for smartphone users, researchers reformulate questionnaire items multiple times during the collection of questionnaire data from students. This is because some experts find it challenging to comprehend the structure of sentences employed in questionnaire items. In such cases, the process of collecting questionnaire data is time-consuming and laborious.
2) The model proposed is theoretical and has not been tested on any application system. Due to the required testing time and effort, the actual testing cannot be included in this research.

6.5 Recommendation for Future Works

As a result of the research conducted, a few suggestions can be taken as a basis for future exploration and it is recommended to explore these suggestions further. By considering the broad scope of the research findings, the potential conclusions can be transformed into numerous publications in the near future.

1) One of the most significant future projects is the demonstration application and testing of the proposed model. Testing could be carried out using the proposed model prototype and run the test in collaboration with students to ensure the robustness of the security techniques.
2) It is possible to adapt the model to other environments, such as user services in banking, telecommunication, and healthcare institutions. The primary security architecture proposed could be implemented in a variety of environments. However, certain modifications to the proposed security strategies could be implemented.
3) The proposed model can be implemented using multiple or hybrid cryptography algorithms such as Elliptic Curve Cryptography (ECC). Using physical biometrics as one of the multiple cryptographies to enhance the user-device authentication model.

6.6 Summary

In conclusion, the purpose of this research was to identify vulnerabilities in security products, particularly for mobile applications, and to address those vulnerabilities in smartphone applications. All research questions were satisfactorily resolved, providing insight into the primary contribution of this research, which is the design of User-Device Authentication Model with Digital Certificate for the

Smartphone User. The implementation of both user authentication and device authentication on smartphones offers a comprehensive security solution that safeguards both the user's personal information and the device, resulting in a more secure and organized smartphone experience.

The goal of future user-device authentication efforts should be to balance security, usability, and privacy while responding to new threats and technologies emerging in the mobile environment. To drive innovation and improve smartphone security, collaboration between researchers, industry professionals, and policy makers is essential.