A SECURE PIN-ENTRY METHOD RESISTANT TO SHOULDER-SURFING AND RECORDING ATTACKS

FARID BINBESHR

FACULTY OF COMPUTER SCIENCE
& INFORMATION TECHNOLOGY
UNIVERSITI MALAYA
KUALA LUMPUR

2022

A SECURE PIN-ENTRY METHOD RESISTANT TO SHOULDER-SURFING AND RECORDING ATTACKS

FARID BINBESHR

THESIS SUBMITTED IN FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF DOCTOR OF PHILOSOPHY

FACULTY OF COMPUTER SCIENCE
& INFORMATION TECHNOLOGY
UNIVERSITY OF MALAYA
KUALA LUMPUR

2022

UNIVERSITI MALAYA

ORIGINAL LITERARY WORK DECLARATION

Name of Candidate: Farid Salem Saeed Binbeshr

Registration/Matric No.: WVA170030

Name of Degree: Doctor of Philosophy

Title of Thesis: Secure PIN-Entry Method Resistant to Shoulder-Surfing and Recording Attacks

Field of Study: Computer Security (Computer Science)

I do solemnly and sincerely declare that:

(1) I am the sole author/writer of this Work;
(2) This work is original;
(3) Any use of any work in which copyright exists was done by way of fair dealing and for permitted purposes and any excerpt or extract from, or reference to or reproduction of any copyright work has been disclosed expressly and sufficiently and the title of the Work and its authorship have been acknowledged in this Work;
(4) I do not have any actual knowledge nor do I ought reasonably to know that the making of this work constitutes an infringement of any copyright work;
(5) I hereby assign all and every rights in the copyright to this Work to the University of Malaya ("UM"), who henceforth shall be owner of the copyright in this Work and that any reproduction or use in any form or by any means whatsoever is prohibited without the written consent of UM having been first had and obtained;
(6) I am fully aware that if in the course of making this Work I have infringed any copyright whether intentionally or otherwise, I may be subject to legal action or any other action as may be determined by UM.

Candidate's Signature Date: May 19, 2022

Subscribed and solemnly declared before,

Witness's Signature Date: May 19, 2022

Name:

Designation:

A SECURE PIN-ENTRY METHOD RESISTANT TO SHOULDER-SURFING AND RECORDING ATTACKS

ABSTRACT

The regular PIN-entry method has been considered the most common method of authentication for systems and networks. However, PINs are easy to be captured through shoulder-surfing and recording attacks. An adversary may shoulder surf the authentication session to obtain the PIN. He or she may use a video-recording device to record a user while performing authentication and later reproduce the PIN. It is also possible that the adversary might install spyware on the compromised device and capture the user input and screen content. This problem with the regular PIN-entry method could be attributed to the involuntary nature of entering the original PIN during authentication. A plethora of PIN-entry methods have been proposed in the literature to mitigate such attacks. They are categorised into direct input and indirect input methods according to the way of entering the original PIN. Unfortunately, these methods either provide no protection against shoulder-surfing and recording attacks (video-based and spyware-based) or hamper the PIN-entry method's usability or compatibility. In this research, an indirect input method that employs the challenge-response approach is proposed in order to produce a One Time PIN (OTP) that obscures the original PIN. Three versions of the proposed PIN-entry method are designed. Two user studies were conducted; preliminary and primary. The preliminary user study was used to find the best version of the proposed PIN-entry method. The primary user study was used to evaluate the security and usability of the best version and compared it with the related work. The results of the user study manifest that the proposed PIN-entry method provides better security than the existing PIN-entry methods while maintaining an acceptable level of usability. Moreover, the user feedback fully

supports the use of the proposed PIN-entry method in critical-security situations.

Keywords: PIN, Password, authentication, shoulder surfing, recording attack.

KAEDAH KEMASUKAN PIN SELAMAT TAHAN TERHADAP SELANCAR BAHU DAN RAKAMAN SERANGAN

ABSTRAK

Penggunaan PIN telah dianggap sebagai kaedah pengesahan identiti yang paling biasa digunakan bagi pengguna sistem dan rangkaian. Walau bagaimanapun, penggunaan PIN amat mudah untuk dipintas melalui serangan keselamatan seperti intipan bahu dan rakaman. Seseorang penyerang itu boleh mengintip di sebalik bahu sewaktu sesi pengesahan untuk mendapatkan PIN. Seseorang penyerang itu juga boleh menggunakan peranti rakaman video untuk merakam pengguna semasa melakukan pengesahan dan mendapatkan PIN daripada rakaman tersebut. Terdapat juga kemungkinan di mana sesorang penyerang itu memasang perisian pengintip pada peranti mangsa dan seterusnya memintas input pengguna dan kandungan skrin. Masalah dengan kaedah kemasukan PIN biasa ini boleh dikaitkan dengan sifat memasukkan PIN asal secara tidak sengaja semasa pengesahan. Banyak kaedah kemasukan PIN telah dicadangkan untuk mengurangkan serangan sedemikian dan boleh dikategorikan kepada kaedah input langsung dan input tidak langsung mengikut cara memasukkan PIN asal. Walau bagaimanpun, kaedah-kaedah ini tidak memberikan perlindungan terhadap serangan intipan bahu dan rakaman (berasaskan video dan perisian intip) atau menjejaskan kebolehgunaan atau keserasian kaedah kemasukan PIN. Dalam penyelidikan ini, kaedah input tidak langsung yang menggunakan pendekatan jawapan-cabaran dicadangkan untuk menghasilkan PIN satu kali (OTP) yang mengaburkan PIN asal. Penyelidikan ini telah mereka bentuk tiga versi kaedah kemasukan PIN. Dua kajian pengguna telah dijalankan iaitu kajian awal dan utama. Kajian pengguna awal telah digunakan untuk mencari versi terbaik kaedah kemasukan PIN yang dicadangkan. Kajian pengguna utama digunakan untuk menilai keselamatan

dan kebolehgunaan versi terbaik dan membandingkannya dengan kerja yang berkaitan. Hasil kajian pengguna menunjukkan bahawa kaedah kemasukan PIN yang dicadangkan memberikan keselamatan yang lebih baik daripada kaedah kemasukan PIN sedia ada di samping mengekalkan tahap kebolehgunaan yang boleh diterima. Selain itu, maklum balas pengguna menyokong sepenuhnya penggunaan kaedah kemasukan PIN yang dicadangkan dalam situasi keselamatan kritikal.

Kata kunci: PIN, Kata laluan, pengesahan, melayari bahu, merakam serangan.

ACKNOWLEDGEMENTS

First and foremost, I would like to praise Allah the Almighty, the Most Gracious, and the Most Merciful for His blessing given to me during my PhD study and in completing this thesis.

I would like to express my sincere gratitude to my supervisors, Prof. Miss Laiha, Dr. Por Lip Yee, and Dr. Aws, for their prompt, insightful, valuable, and frank feedback on my research. I deeply appreciate their willingness to help me whenever I had difficulties during my study.

I would like to extend my sincere gratitude to my parents, wives, daughters, brothers, and sisters for their love, support, and encouragement in achieving this research work.

I would like to thank Eng. Abdullah A. Bugshan, Hadhramout Foundation, Hadhramout University, University Malaya, Yemen Cultural Attache and Yemen Embassy in Malaysia, Yemen Ministry of Higher Education and Scientific Research for their financial and administrative support.

Special thanks go to my friends, colleagues, and all persons who helped me during my study.

TABLE OF CONTENTS

Abstract iii

Abstrak v

Acknowledgements vii

Table of Contents viii

List of Figures xii

List of Tables xiv

CHAPTER 1: INTRODUCTION 1

1.1 Background 1

1.2 Problem Statement 3

1.3 Research Objectives 5

1.4 Research Questions 6

1.5 Scope of Research 6

1.6 Significance of the Research 7

1.7 Organisation of the Thesis 8

CHAPTER 2: LITERATURE REVIEW 10

2.1 Introduction 10

2.2 Shoulder-Surfing and Recording Attacks in PIN-Entry Method 10

2.2.1 Shoulder-Surfing Attack 10

2.2.2 Recording Attacks 11

2.2.2.1 Video-Based Recording Attack 11

2.2.2.2 Spyware-Based Recording Attack 12

2.3 PIN-Entry Methods and Usability 13

2.4 PIN-Entry Methods Resistant to Shoulder-Surfing and Recording Attacks 13
2.4.1 Direct Input Methods 15
2.4.1.1 Gaze-Based Methods 15
2.4.1.2 Visual Distraction Methods 22
2.4.2 Indirect Input Methods 26
2.4.2.1 Challenge-Response Methods 26
2.4.2.2 Other Indirect Input Methods 41
2.5 Related Work 42
2.6 Chapter Summary 51

CHAPTER 3: RESEARCH METHODOLOGY 56

3.1 Introduction 56
3.2 Research Methodology Framework 56
3.2.1 Phase1: Systematic Literature Review (SLR) 56
3.2.1.1 Planning Stage 57
3.2.1.2 Conducting Stage 60
3.2.1.3 Reporting Stage 62
3.2.2 Phase2: Proposed PIN-Entry Method Design 69
3.2.3 Phase3: Prototype Implementation 71
3.2.4 Phase4: Evaluation and Analysis 71
3.3 Chapter Summary 73

CHAPTER 4: PROPOSED PIN-ENTRY METHOD 74

4.1 Introduction 74
4.2 Overview of the Proposed PIN-entry Method 74
4.3 Versions of the Proposed PIN-entry Method 75

4.3.1 Registration Process: 75
4.3.2 Login Process: 76
4.3.2.1 First version 76
4.3.2.2 Second version 77
4.3.2.3 Third version 79
4.3.2.4 Error attempts 81
4.4 Prototype Implementation of the Proposed PIN-Entry Method 82
4.4.1 Use Case Diagram of the Proposed PIN-Entry Method 82
4.4.2 Database Design 83
4.5 Chapter Summary 84

CHAPTER 5: PRELIMINARY USER STUDY 86

5.1 Introduction 86
5.2 Experimental Settings 86
5.3 Participants 87
5.4 Procedure 88
5.5 Security Analysis 89
5.6 Usability Analysis 90
5.7 User feedback 92
5.8 Chapter Summary 92

CHAPTER 6: PRIMARY USER STUDY 95

6.1 Introduction 95
6.2 Experimental Settings 95
6.2.1 Participants and Procedure 95
6.3 Security Analysis 96

6.3.1 Shoulder-surfing Attack 96
6.3.2 Video-Based Recording Attack 97
6.3.3 Spyware-Based Recording Attack 98
6.3.4 Guessing Attack 100
6.3.5 Custom Settings 100
6.4 Usability Analysis 102
6.4.1 PIN-Entry Time 103
6.4.2 Error Rate 104
6.4.3 Learning Effect 104
6.5 User Feedback 105
6.6 Comparison With Related Work 107
6.7 Chapter Summary 108

CHAPTER 7: CONCLUSION 110

7.1 Objectives 110
7.2 Contributions 112
7.3 Limitations and Future Directions 113
References 117
List of Publications and Papers Presented 128

LIST OF FIGURES

Figure 2.1: Authentication methods Taxonomy 14

Figure 2.2: Taxonomy of PIN-entry methods resistant to shoulder-surfing and recording attacks 16

Figure 3.1: Research Methodology Framework 57

Figure 3.2: Study Selection Process 64

Figure 4.1: Login Phase 76

Figure 4.2: The keypad of the first version of the proposed PIN-entry method 77

Figure 4.3: The keypad of the second version of the proposed PIN-entry method 79

Figure 4.4: The keypad of the third version of the proposed PIN-entry method 80

Figure 4.5: Use case diagram of the proposed PIN-entry method 83

Figure 5.1: Shoulder-surfing attack success rate on easy and hard PINs of the three versions of the proposed PIN-entry method 89

Figure 5.2: Recording attacks success rate on easy and hard PINs of the three versions of the proposed PIN-entry method 91

(a) Success rate of video-based recording attack 91

(b) Success rate of spyware-based recording attack 91

Figure 5.3: PIN-entry time for easy and hard PINs of the proposed PIN entry method versions 94

Figure 5.4: Basic error rate for easy and hard PINs of the proposed PIN entry method versions 94

Figure 6.1: Attack success rate for easy and hard PINs of the proposed PIN-entry method. 97

Figure 6.2: Success rate of shoulder-surfing, video-recording, and spyware attacks over three captured authentication sessions 99

(a) Easy PINs 99

(b) Hard PINs 99

Figure 6.3: PIN-entry time for easy and hard PINs of the proposed and regular PIN-entry methods 103

Figure 6.4: Basic error rate for easy and hard PINs of the proposed and regular PIN-entry methods. 104

Figure 6.5: Variations in PIN-entry time over 10 trials using easy and hard PINs of the proposed and regular PIN-entry methods. 105

Figure 6.6: Participants' feedback of the proposed PIN-entry method in terms of ease of use, usage, and security. 106

LIST OF TABLES

Table 2.1: A summary of gaze-based PIN-entry methods 23

Table 2.2: A summary of visual distraction PIN-entry methods..... 27

Table 2.3: A summary of audio-based challenge-response PIN-entry methods 34

Table 2.4: A summary of haptic-based challenge-response PIN-entry methods 40

Table 2.5: A summary of the related work PIN-entry methods 52

Table 2.5: A summary of the related work PIN-entry methods (cont.)..... 53

Table 2.5: A summary of the related work PIN-entry methods (cont.)..... 54

Table 3.1: Quality Assessment Criteria (Keele et al., 2007; Programme, 2019)..... 60

Table 3.2: Data extraction from 61

Table 3.3: Search fields and filters for each database..... 62

Table 3.4: Research methods used by selected studies 66

Table 3.5: Participants Demographic Information Form 72

Table 4.1: Database metadata..... 84

Table 5.1: PIN Types and Patterns 87

Table 6.1: Recording attacks against 6-digit PINs entered through the proposed PIN-entry method..... 102

Table 6.2: Comparison of PIN-entry Methods..... 107

Table 6.3: Level of resistance of a PIN-entry method against shoulder-surfing and recording attacks (Binbeshr et al., 2020)..... 108

CHAPTER 1: INTRODUCTION

1.1 Background

Digital technology has been essential for individuals, businesses, and governments in order to pursue their rising range of activities. Digital technology includes all computer systems, devices, services, tools, and other resources that generate and process data. Unfortunately, unauthorised access to these resources has become so widespread with the rise in the use of digital technology. One of the most important access controls and front-line defences against unauthorised access to computer resources is authentication. Overall, authentication is the process of confirming the identity of a user, device, or other entity as a prerequisite in order to access a system or service (Greene, Franklin et al. 2016). There are two types of authentications: machine authentication and user authentication. Machine authentication is responsible for verifying the identity of a machine. It does not provide any assurance with regard to the person that runs or uses the machine. This is the responsibility of the user authentication. Therefore, user authentication can be defined as the process of verifying the identity of a user (O'Gorman, 2003). In this thesis, the focus is on user authentication methods.

Generally, user authentication methods are classified into token-based, biometric-based, and Knowledge-based (De Zheng, 2011; O'Gorman, 2003). In token-based authentication, a user should present a token such as a bankcard to be authenticated. Tokens are physical devices that store static information like passwords, or they dynamically generate a One Time PIN (OTP) password that is valid for a single login session or transaction. In biometric-based authentication, a user makes use of his or her unique characteristics such as a fingerprint, to perform authentication (Aljaffan, 2017; O'Gorman, 2003). In knowledge-based authentication, a user enters a shared secret to prove his or her identity

(Biddle et al., 2012).

The knowledge-based or password-based authentication method is classified into graphical and textual (Suo et al., 2005). In the graphical password method, a picture or sketch is used as a password for authentication instead of text. The reason behind using pictures is that humans can remember pictures easier than texts (Shepard, 1967). Graphical password methods, however, are not widely used in practice, and they have reliability and storage issues (Suo et al., 2005). On the contrary, the textual password method is still the most common method of authentication for services and systems because of its convenience and inexpensive cost (Herley et al., 2009; Stamp, 2011). In textual-based password methods, users utilise text, digits, special symbols, or all to set their passwords (Aljaffan, 2017). Personal Identification Number (PIN) is an example of the textual-based password method that utilises only digits.

In 1967, the PIN was invented by James Goodfellow for the Chubb Integrated System as a secure automated method to dispense cash (Konheim, 2016). With the rapid development of digital technologies, PIN has proliferated in various embedded devices and applications as a secure method against unauthorised access. The continuous usage of PIN in everyday life and its applicability in resource-limited environments keeps it a prevailing method for user authentication (Papadopoulos et al., 2017; Wang et al., 2017).

The PIN, or regular PIN-entry method, is widely used in daily authentication for many services and systems despite the presence of other alternatives. For example, the regular PIN is used as a personal method of authentication to unlock smart device screens, withdraw cash from Automated Teller Machines (ATMs), make payments at the Point Of Sale (POS) systems, and open electronic doors (Chakraborty & Mondal, 2014; Nyang et al., 2018; Von Zezschwitz et al., 2015). The PIN is a special kind of knowledge-based or password authentication methods, composed only of digits and is typically 4-6 characters. The

widespread adoption of the regular PIN-entry method is due to the ease of remembering and entering the PIN (Greene et al., 2016). Shen et al. (2016) conducted a study on 6 million passwords and found that most of these passwords are composed of only digits or numbers. The PIN does not require any letters or special symbols. The short length of PINs makes them easier to remember than other knowledge-based authentication methods, and the composing of only digits makes them easier to enter. Therefore, PINs are recognised as less error prone and suitable for virtual and physical resource-limited environments that require a numpad rather than the standard keyboard (Malkin et al., 2017; Wang et al., 2017).

1.2 Problem Statement

It is noteworthy to mention that although PIN or the regular PIN-entry method is widely used in daily authentication, it is often easy to be captured though simple and effective attacks such as shoulder-surfing and recording attacks (both video-based and spyware-based). In shoulder-surfing attacks, the attacker uses his or her naked eye to capture the authentication session, whereas he or she utilises a recording tool in the recording attacks. The problem of shoulder-surfing and recording attacks arises when an attacker observes a login PIN directly or using a recording tool and later reproduces the PIN (Ku et al., 2016; Nyang et al., 2018). The reason for this problem is that users reveal their original PINs at each authentication session (Still & Bell, 2018). In other words, the same PIN is used every time by users when they login into a system or service and never automatically changes over time. Thus, shoulder-surfing or recording attackers need to know the user's PIN once in order to use it in subsequent transactions.

Shoulder-surfing and recording attacks are simple and efficient attacks against the regular PIN-entry method (Souza et al., 2018). A real word incident of such attacks has been discussed by Hirakawa et al. (2015). They reported an incident of video-based recording

attacks against ATM PIN passwords in Japan. The attackers had installed video cameras at different ATM locations in the city of Tokyo. The bank authorities have investigated the incident and declared that more than 60 ATMs have been captured by concealed video cameras in the city. According to an online study (260 participants) conducted by Harbach et al. (2014), 35% of the participants reported their concerns about observing them while unlocking their smartphones and stealing their PINs. In the field study (52 participants), 17% of the participants perceived that they were targeted by shoulder-surfing attacks during an authentication session. Davin et al. (2017) conducted a user study about analysing the resilience of the regular PIN-entry method used to unlock smartphones against everyday shoulder-surfing attacks. The study results found that the lowest success rate of shoulder-surfing attacks against unlocking smartphone 6-digits PIN-entry method is 10.9% (Davin et al., 2017, as cited in Li et al., 2017). This percentage is expected to be higher for both video-based and spyware-based recording attacks.

Many PIN-entry methods have been proposed in the literature to solve the problem of shoulder-surfing and recording attacks associated with regular PIN-entry method. These methods can be classified into direct and indirect input methods according to whether a user enters the original PIN or not (Binbeshr et al., 2020). Direct input methods ask users to reveal the original PIN during authentication, just as the regular PIN-entry method does. However, these methods try to disguise the observer from capturing the original PIN through gaze input (Carneiro et al., 2019; Ibrahim & Ambreen, 2019; Kumar et al., 2019) and visual distraction (Guerar et al., 2019; Kabir et al., 2020; Krombholz et al., 2016; Nandhini & Jayanthy, 2019; Still & Bell, 2018; Sugumar & Soundararajan, 2017). Despite reducing the shoulder-surfing effect, direct input methods are still vulnerable to recording attacks (video-based or spyware-based). Indirect input methods prevent users from entering the original PIN during authentication through a challenge-response approach. That is, a

challenge is sent to the user, and then he or she finds out and enters the response based on his or her knowledge of the challenge and the original PIN. The indirect input methods can be categorised into audio-based (Dan & Ku, 2017; Perković, Čagalj, & Saxena, 2010; Rajarajan et al., 2018), haptic-based (Chakraborty et al., 2016; M.-K. Lee, Nam, & Kim, 2016), and visual-based (Kasat & Bhadade, 2018; Kwon & Na, 2015; Roth et al., 2004; Von Zezschwitz et al., 2015), according to the channel through which the challenge is sent. Nonetheless, these indirect input methods either provide no protection against recording attacks or hamper the usability, compatibility or both of the PIN-entry method (Souza et al., 2018).

It could be argued that physiological biometric authentication methods, such as fingerprints, can solve this problem. Besides, users favour biometric authentication methods over the PIN-entry method (Breitinger et al., 2020). Nonetheless, biometric methods are still error-prone, costly, and unchangeable once leaked (Yadav et al., 2015). Furthermore, the PIN-entry method is used by most devices for fallback authentication when biometrics fail. Consequently, an attacker can resort to the fallback authentication method to detour biometric verification (Van Nguyen et al., 2017). Therefore, the development of a secure and usable PIN-entry method against such attacks would be promising.

1.3 Research Objectives

This research aims to improve the security of the regular PIN-entry method so as to mitigate shoulder-surfing and recording attacks. The objectives of this research are listed as follows:

1. To review the existent PIN-entry authentication methods resistant to shoulder-surfing and recording attacks.
2. To propose a PIN-entry method that resists shoulder-surfing and recording attacks.

3. To develop a prototype of the proposed PIN-entry method.
4. To evaluate the effectiveness of the proposed PIN-entry method in terms of resisting shoulder-surfing and recording attacks using quantitative/qualitative to measure.

1.4 Research Questions

This research has answers to the following questions:

1. What are the existing PIN-entry methods resistant to shoulder-surfing and recording attacks in the literature?
2. How does the proposed PIN-entry method resist shoulder-surfing and recording attacks?
3. How can the proposed PIN-entry method be developed?
4. How can the proposed PIN-entry method be evaluated in terms of resisting shoulder-surfing and recording attacks?

1.5 Scope of Research

In order to achieve the research objectives stated in section 1.4 within the stipulated timeframe, the scope of research is focused only on PIN-entry methods resistant to shoulder-surfing and recording attacks (video-based and spyware-based). This excludes other knowledge-based authentication methods like passwords because they contradict the usability of the PIN with respect to password length and composition. Other authentication systems, like biometric-based and token-based methods, are not under consideration as well. These methods are excluded because they have serious limitations, in addition to the cost and convenience concerns. Biometric methods need to accept some level of acceptable errors to reduce the false rejection rate. Also, a biometric device is required to capture the data, which is not always available. For tokens, they normally require another authentication factor such as a PIN for further protection against steal or loss (Aljaffan,

2017; Wang et al., 2016). This also excludes PIN-entry methods that are hybrid or require additional channel (audio or habtic) of communication because they do not satisfy the PIN's desirable requirements of being easy and fast (Nyang et al., 2018). This research is limited to the registration and login phases. That is, storing and transferring the credentials is out of the scope of the research.

This research focuses on shoulder-surfing, video-based recording, and spyware-based recording attacks because they are a major threat against PIN-entry authentication methods. In particular, shoulder-surfing and video-based recording attacks are easy to conduct, and they do not require any sophisticated devices or skills (Khan et al., 2018). For example, an attacker can stand close to a victim in a public place and capture the PIN using his or her eyes or a smartphone camera without attracting the victim's attention. The possibility of capturing the PIN is highly likely due to its short length (4-6 numerical characters) and simplicity (10-digit keypad). The spyware-based recording attack is a much more advanced and threatening recording attack that discloses user input and screen content during the authentication process. Therefore, this attack is included in this research in order to confirm the robustness of a PIN-entry method in resisting shoulder-surfing and other recording attacks by confirming its robustness in resisting spyware-based recording attacks.

1.6 Significance of the Research

This research aims to improve the security of the regular PIN-entry method in terms of resisting shoulder-surfing and recording attacks. An indirect input PIN-entry method that employs a challenge-response approach is proposed. The challenge-response approach relies on the addition mod 10 with a mini-challenge keypad in order to produce a OTP password that obscures the original PIN. The use of addition mod 10 generates equally likely OTP digits, removing any correlation between authentication sessions, and thereby

resisting shoulder-surfing and recording attacks. The proposed PIN-entry method could be the best alternative to the regular PIN-entry method for those who expect a high level of security for their services. It could also be utilised by users to secure a variety of everyday life applications and services. Moreover, three different versions of the proposed PIN-entry method have been designed. These variation designs of the proposed PIN-entry method could provide alternative ways for researchers and developers who are interested in exploring and developing a secure and usable PIN-entry method.

This research work includes a Systematic Literature Review (SLR) of the existing PIN-entry methods resistant to shoulder-surfing and both video-based and spyware-based recording attacks. The conducted SLR would be valuable to the cyber security community, researchers, practitioners, developers, and users in that it enhances the knowledge about the security and usability issues on PIN-entry methods. It raises awareness of the importance of being prepared with appropriate solutions for these issues. This SLR also provides baseline information on the up-to-date status of PIN-entry methods resistant to shoulder-surfing and recording attacks. This includes a taxonomy of the existing PIN-entry methods, in addition to the research methods and evaluation metrics that were used to evaluate these PIN-entry methods.

1.7 Organisation of the Thesis

This thesis consists of seven chapters. The first chapter discusses the introduction of the thesis. It provides a brief background on PIN-entry authentication methods. It also describes the problem statement and identifies the research objectives, research questions, and scope of this thesis. The significance of this research work is stated in this chapter.

Chapter 2 presents the literature review of this research work. It covers the background knowledge of the PIN-entry method, shoulder-surfing, and recording (video-based and spyware-based) attacks. This chapter also summarises the current state of knowledge and

limitations of the PIN-entry methods resistant to shoulder-surfing and recording attacks.

The research methodology undertaken to achieve the research objectives of this thesis is described in Chapter 3. It presents a framework of four phases; each phase details the methods and outcomes associated with a research objective.

Chapter 4 describes the proposed PIN-entry method resistant to shoulder-surfing and recording attacks. It provides an overview of how the proposed PIN-entry method resists shoulder-surfing and recording attacks. Three versions of the proposed PIN-entry method and their implementation details are discussed in this chapter.

The preliminary and primary user studies are discussed in Chapter 5 and Chapter 6, respectively. The preliminary user study was conducted to find the best version of the proposed PIN-entry method, whereas the primary user study was conducted to evaluate the security and usability of the best version of the proposed PIN-entry method and compare it with the regular one and related work. The experiment settings, security analysis, usability analysis, and user feedback are discussed in each chapter. Chapter 6 also compares the proposed PIN-entry method to the work done by other people.

Chapter 7 concludes this thesis. It discusses the research objectives achieved and highlights the main contributions of this research work. The limitations and future directions have been stated as well.

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

This chapter reviews the literature relevant to PIN-entry methods resistant to shoulder-surfing and recording attacks (video-based and spyware-based). It begins by providing background information about shoulder-surfing and recording attacks, including video-based and spyware-based. A taxonomy of the PIN-entry methods resistant to shoulder-surfing and recording attacks is presented. These PIN-entry methods are mainly categorised into direct input and indirect input methods. These categories and their sub-categories are summarised. This chapter discusses the related work before presenting the chapter summary.

2.2 Shoulder-Surfing and Recording Attacks in PIN-Entry Method

The rise in popularity of PINs makes them susceptible to many attacks, including shoulder-surfing, video-based recording, spyware-based recording, smudge, replay, phishing, and guessing attacks. Shoulder-surfing and recording attacks (both video-based and spyware-based) are a major threat against PIN-entry methods due to their simplicity and effectiveness. This research work only focuses on shoulder-surfing and recording attacks (video-based and spyware-based).

2.2.1 Shoulder-Surfing Attack

Shoulder-surfing is one of the simple and efficient attacks that has acted as an underlying motive behind many works conducted in the area of usable security (Eiband et al., 2017). As the name implies, the shoulder-surfer obtains sensitive information by looking over the user's shoulder without his or her consent. This sensitive information includes PIN authentication session details and other personalised content. This thesis focuses on a shoulder-surfing attack against the user's PIN authentication session details.

Shoulder-surfing is a potential threat to PINs in crowded and public places such as trains, airports, Internet cafés, and markets. It is relatively easy for shoulder surfers to stand close to a victim in such places without being noticed. In this type of attack, the attacker uses his or her naked eye to capture the authentication session data. Victims are usually unaware of the act of shoulder surfing, according to real stories collected from both victims and shoulder surfers (Eiband et al., 2017). The analysis of the real stories revealed the negative feelings of both victims and observers toward the shoulder-surfing act.

2.2.2 Recording Attacks

Recording attacks resemble shoulder-surfing attacks in which the attacker tries to observe the authentication session data in order to recover the original PIN. The attacker, however, makes use of a recording hardware or software tool to record the authentication session data. The recording attacks are classified into video-based and spyware-based recording attacks according to the way that is used to record the authentication session data.

2.2.2.1 Video-Based Recording Attack

In this attack, the attacker employs a camera device in order to record the user's authentication session multiple times. The attacker may use a tiny hidden camera, video surveillance, or mobile phone in order to record the PIN entry authentication process. Later, he or she watches these recordings and reproduces the original PIN.

The effectiveness of video-based recording attacks against PIN-entry authentication methods is much more higher than the effectiveness of shoulder-surfing attacks. In fact, the shoulder surfer makes use of his or her cognitive capabilities so as to observe and memorise the PIN entry authentication session. Thus, the accuracy of capturing the PIN entry authentication session is limited by the cognitive capabilities of the human beings

(Miller, 1956; Vogel & Machizawa, 2004). On the contrary, the attacker that employs the video-based recording attack improves the accuracy of his or her observation of the PIN entry authentication session with the aid of the video recording device.

The susceptibility of video-based recording attacks is not a purely theoretical and trivial matter. There were cases in which the video-based recording attack has been employed by hackers in order to record sensitive information (Scroxton, 2022; P. P. Shi, 2010; Wang et al., 2017). Moreover, the unawareness of such an attack makes it extremely harder to be avoided by the victims. Therefore, video-based recording attack is a serious threat to the security of PIN authentication systems and other sensitive information.

2.2.2.2 Spyware-Based Recording Attack

Generally, spyware is malicious software that is designed to monitor and gather a user's data without his or her consent and forward it to a third-party (Egele et al., 2007). Spyware exists in different types and for different purposes. Kaspersky (Kaspersky, 2022) classifies spyware into trojan spyware, adware, tracking cookies files spyware, and system monitoring spyware. The trojan spyware is a malicious trojan that takes the delivery of the spyware software. The adware is designed to monitor users' data and sell them to advertisers. The spyware that tracks users when surfing the internet is called tracking cookies files spyware. The system monitoring spyware functions as an activity tracker for what a user does on a computer in order to record sensitive information such as login usernames and passwords, PINs, credit card numbers, emails, and more. Keyloggers, touchloggers, and spyware-based recording are categorised under the system monitor spyware. This research focuses on spyware-based recording attacks that leak the information exchanged during the authentication session, including user input and screen content.

PIN-entry authentication methods are more threatened by spyware-based recording attacks than shoulder-surfing and video-based recording attacks. A user may physically

attempt to shield the screen from observers in order to defend against shoulder-surfing and video-based recording attacks; however, the physical shield is not going to be useful in the case of defending against spyware-based recording attacks. Therefore, if a PIN-entry method is confirmed to be resistant to spyware-based recording attacks, it is undoubtedly resistant to shoulder-surfing and other recording attacks (T. Kim et al., 2014).

2.3 PIN-Entry Methods and Usability

Usability is a highly critical component of designing a secure PIN-entry method. In fact, users tend to use a simple PIN-entry authentication method even though it may affect the security. Usability is mainly measured by the speed of performance (i.e., PIN-entry time) and the error rate by users (Binbeshr et al., 2020). Thus, these two measures are taken into account to figure out how usable an existing PIN-entry method resistant to shoulder-surfing and recording attacks in the literature. Usable PIN-entry methods should enable users to perform authentication within 10 seconds with a success rate of 90% (Chakraborty et al., 2019).

2.4 PIN-Entry Methods Resistant to Shoulder-Surfing and Recording Attacks

As shown in Figure 2.1, authentication methods are classified into biometric-based (something you are), token-based (something you have), and knowledge-based (something you know) (De Zheng, 2011; O'Gorman, 2003). The biometric-based authentication method relies on the unique characteristics of an individual to perform authentication. These unique characteristics include finger or palm prints, facial features, iris or retina features, and voice features. Token-based authentication works by ensuring that a user presents a token, such as a credit card, to be authenticated. The knowledge-based authentication method, also known as password-based authentication, authenticates a user based on his or her knowledge of a shared secret. The knowledge-based authentication methods

are classified into textual and graphical. Textual methods use texts for authentication, whereas pictures or sketches are used by graphical methods. The textual methods can be classified into alphanumeric, passphrase, and PIN. An alphanumeric password is a string of letters, digits, and symbol characters. For added security, the passphrase is a sequence of words that is longer than an alphanumeric password. The PIN, or PIN-entry method, is a textual password consisting of only 4-6 digits. This research work is limited to the PIN as described in Section 1.5.

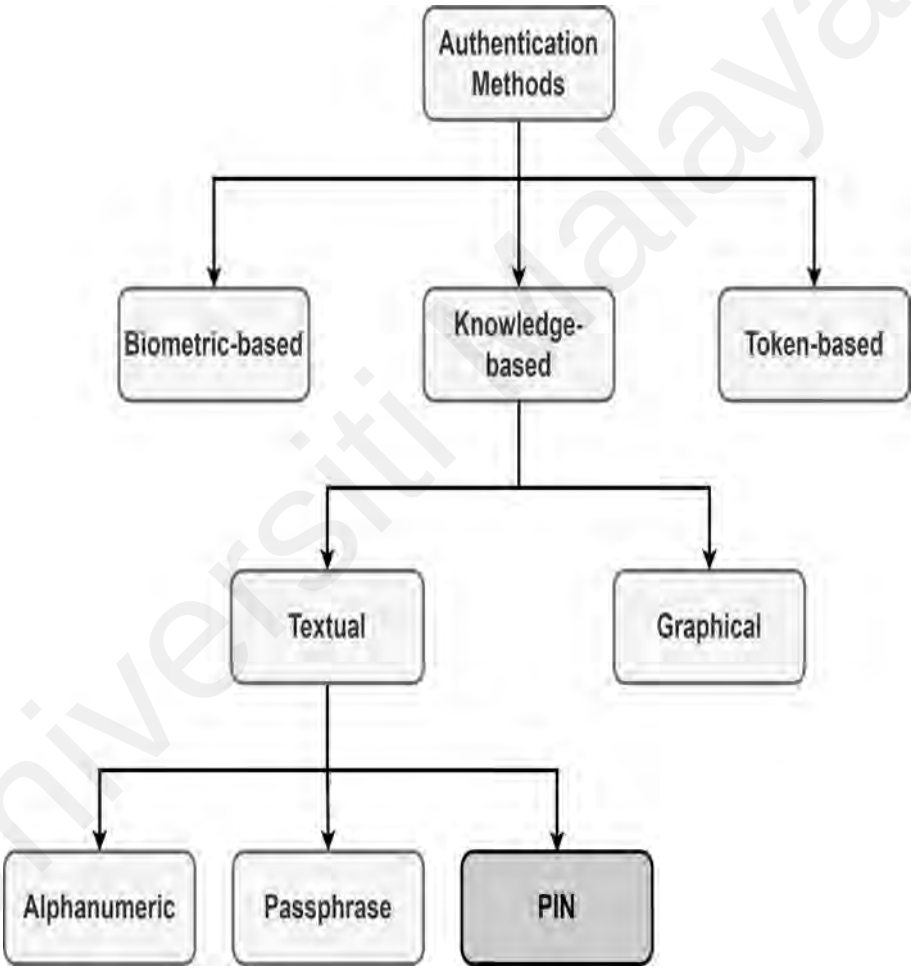


Figure 2.1: Authentication methods Taxonomy

PIN-entry methods resistant to shoulder-surfing and recording attacks are generally classified into either direct or indirect input. In direct input methods, users reveal the original PIN during the authentication process. By contrast, indirect input methods prevent users from entering the original PIN directly (Gugenheimer et al., 2015; Still & Bell,

2018). Figure 2.2 shows the taxonomy of the existing PIN-entry methods resistant to shoulder-surfing attack. The level of resistance of each PIN-entry method against shoulder-surfing, video-based recording, and spyware-based recording attacks has been categorised into high, moderate, low, and vulnerable (Binbeshr et al., 2020). A PIN-entry method is marked high when it is fully resistant to multiple observed or recorded authentication sessions. It is marked moderate when it is partially resistant to multiple observed or recorded authentication sessions. A low resistant PIN-entry method only combats a single observed or recorded authentication session. The PIN-entry method that is not resistant to any observed or recorded authentication session is marked as vulnerable.

2.4.1 Direct Input Methods

Previous research has shown that direct input methods attempt to disguise the observer from obtaining the original PIN through gaze input and visual distraction approaches.

2.4.1.1 Gaze-Based Methods

Gaze-based methods (Almoctar et al., 2018; Carneiro et al., 2019; Das et al., 2020; Holland & Morelli, 2018; Ibrahim & Ambreen, 2019; Khamis et al., 2017; Kumar et al., 2019; J.-I. Lee et al., 2017; Li et al., 2017; Seetharama et al., 2015; SM et al., 2021; Weaver et al., 2011), enable the use of eyes to enter PINs to minimise the effect of shoulder-surfing attacks caused by direct input interaction (i.e., touch). For example, SM et al. (2021) developed a gaze-based PIN authentication algorithm with an eye blinking mechanism in order to secure the PIN numbers against shoulder-surfing attacks. Face recognition and dynamic keypad mechanisms are also employed for added security. The face recognition mechanism detects the face of a user using the system camera. The user needs to enter his or her PIN using eye blinks on the displayed dynamic keypad. For verification, the entered PIN is compared with the user's PIN in the database. The proposed PIN-entry method can

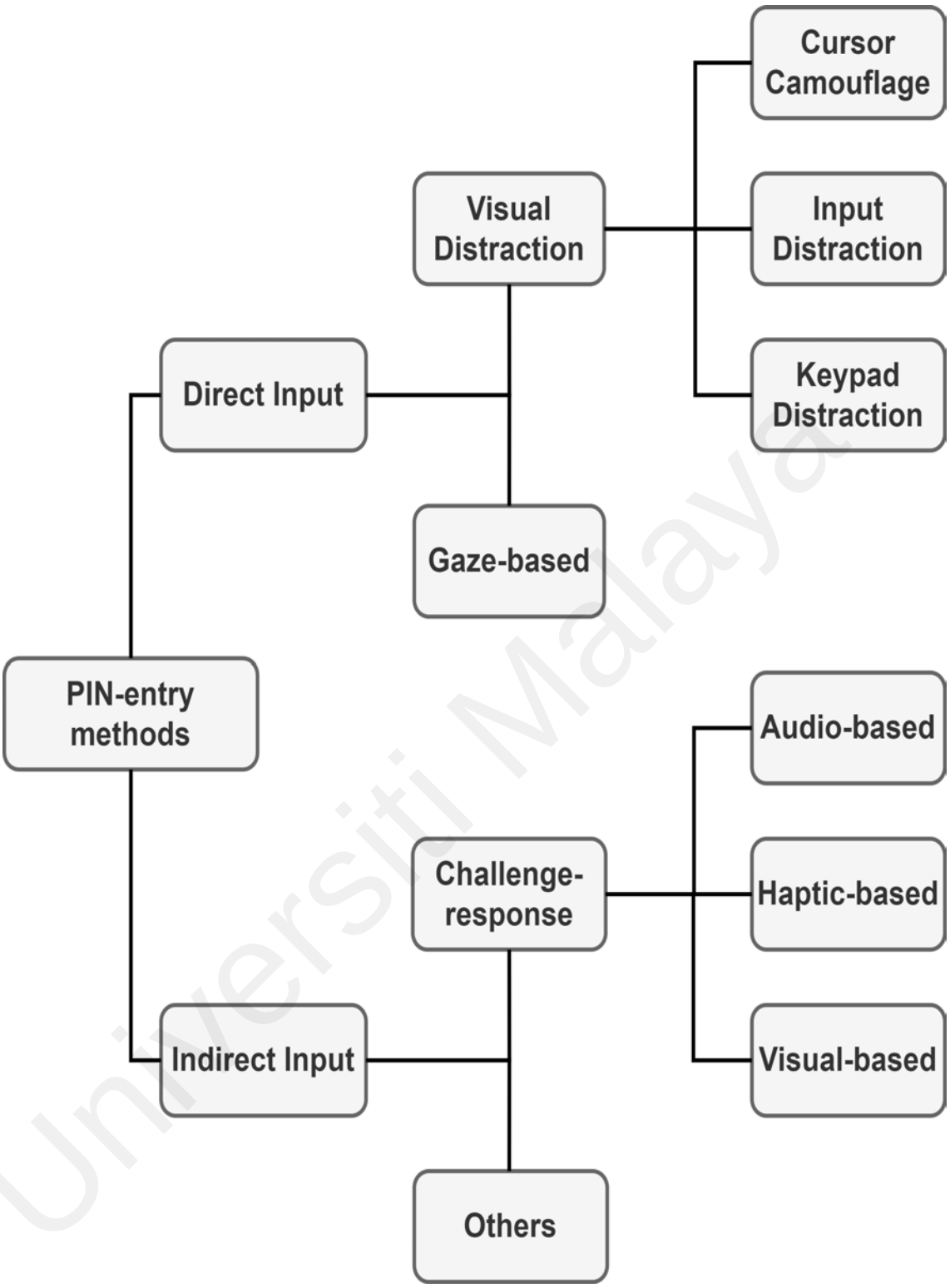


Figure 2.2: Taxonomy of PIN-entry methods resistant to shoulder-surfing and recording attacks

provide a high and moderate resistance against shoulder-surfing and video-based recording attacks. However, it is vulnerable to spyware-based recording attacks. The reported PIN-entry time of the proposed PIN authentication method is too high (65 seconds). The principle of the dynamic keypad was employed by Holland and Morelli (2018) in order to propose a secure PIN authentication method using gaze input.The proposed PIN-entry method advocates the shoulder surfers by shuffling the digits of the keypad used to enter the PIN. This way could provide a high and moderate resistance to shoulder-surfing and video-based recording attacks; however, it is still prone to spyware-based recording attacks. An identified limit of using a dynamic keypad could be the increase in the PIN-entry time and the error rate when a user enters his or her PIN password.

A gaze-based PIN-entry method using eye pupil movement was devised by Das et al. (2020) in order to secure the user's PIN entry against shoulder-surfing attacks. To input the PIN, a user moves his or her eye pupil in different directions (i.e., right, middle, and left), which in turn are transformed or mapped into different patterns of digits (0,1,2, ..., 8, 9). The proposed PIN-entry method makes use of machine learning object detection algorithms such as Haar Cascade and the Histogram of Oriented Gradients (HOG). The Haar Cascade is used for face and eye detection, whereas the HOG algorithm (integrated with SVM classifier) is used for eye blink detection. For pupil detection, canny edge detection and Hough Circle Transform (HCT) algorithms are employed. A projection function algorithm is used for eye pupil tracking (looking right, looking middle, or looking left). The experimental results showed a high accuracy rate for eye pupil detection, eye pupil blink detection, and eye pupil tracking. The study presents some limitations. One limitation of the proposed PIN-entry method, however, is that it was not tested against shoulder-surfing and recording attacks. Another limitation of the proposed PIN-entry method is the high PIN-entry time.

Carneiro et al. (2019) introduced a gaze-based PIN-entry authentication method named PursuitPass in order to protect PIN passwords against shoulder-surfing attacks. PursuitPass is a visual pursuit moving target method with free calibration that requires a user to enter his or her PIN by following the moving digits with his or her eyes. The random movement of the digits adds a liveness feature to the method so as to avoid the recording of the eyes. Two user studies were conducted to evaluate the PursuitPass method. The first study was intended to find the best pattern matching algorithm (out of four) for PursuitPass eye tracking. The second user study was designed to evaluate the performance of the PursuitPass method. PursuitPass is capable to defend against shoulder-surfing and video-based recording attacks; however, it is still prone to spyware-based recording attacks. The findings show that PursuitPass can achieve high accuracy when entering a 4-digit PIN password, with an average PIN-entry time of more than 10 seconds.

To overcome the security limitations of the existing gaze-based PIN-entry, Ibrahim and Ambreen (2019) proposed a multimodel (gaze and touch) PIN authentication method named GazeTouchCrossPIN. The proposed gaze PIN method integrates the touch and gaze gestures in order to key in a PIN password. To illustrate, a user first touches or presses a digit on the keypad to form a cross of digits. The pressed digit is considered the center of the cross. Then, the user needs to gaze in the direction (right, left, top, or bottom) that has the user's PIN digit. Suppose the user pressed on the digit 8 in order to form a cross of digits. This results in having the digit 7 on the left side, the digit 9 on the right side, and the digit 5 on the top side, and the digit 0 on the bottom side. If the user's PIN digit is 9, then he or she is supposed to gaze to the right side. GazeTouchCrossPIN has been evaluated and analysed with respect to PIN-entry time, shoulder-surfing attack, and iterative shoulder-surfing attacks. The reported results of the usability analysis indicate that a user may take roughly 10 seconds to enter his or her PIN

password using GazeTouchCrossPIN. The error rate was not reported. With respect to security analysis, GazeTouchCrossPIN can provide a moderate resistance to get rid of the shoulder-surfing and iterative shoulder-surfing attacks. The video recording attacker may recover the PIN within two recorded sessions; the spyware attacker can get the PIN from the first authentication session.

Kumar et al. (2019) proposed a multimodel gaze-based PIN authentication method named TouchGazePath. TouchGazePath is similar to GazeTouchCrossPIN in which the touch and gaze gestures are employed in order to enter the PIN digits. A user starts entering a PIN by touching at any place on the virtual keypad and does not lift his or her finger. Then, he or she needs to gaze at the keys that contain his or her PIN digits using eyes. After that, the user can lift his or her finger from the virtual keypad. TouchGazePath is supposed to defend against shoulder-surfing attacks because of the difficulty of observing the entered PIN through the eyes. It also may reduce the effect of video-based recording attacks. However, TouchGazePath is susceptible to spyware-based recording attacks. For usability, a user study of 18 participants was conducted to test the error rate and PIN-entry time. The findings of the user study hint that users may enter their PINs fast using TouchGazePath. In spite of the short PINe-entry time, users may need more than one attempt to successfully login. The user feedback confirms that the touch-only input method is better than the touch and gaze or other gaze input methods due to its familiarity.

Similar to TouchGazePath and GazeTouchCrossPIN, Khamis et al. (2017) proposed GazeTouchPIN, a secure gaze-based PIN entry authentication method for mobile devices. GazeTouchPIN employs both gaze gesture and touch input so as to mitigate shoulder-surfing and recording attacks. To perform authentication, a user is asked to select a row of two digits using the touch gesture, and then gaze to left or right in order to enter a PIN digit. The keypad layout of GazeTouchPIN comprises all digits from 0 to 9 distributed in two

columns and five rows. Two user studies were used to test the usability and security of the proposed PIN-entry method. GazeTouchPIN requires a high PIN-entry time and error rate. Thus, it is suggested to be used for an application that requires a high level of security. The security of GazeTouchPIN is comparable with TouchGazePath and GazeTouchCrossPIN in resisting shoulder-surfing, video-based recording, and spyware-based recording attacks.

A shoulder-surfing resistant gaze-based PIN digit entry method named PathWord was proposed byAlmoctar et al. (2018). PathWord relies on the digit shape and eye movement in order to authenticate users. Each digit (0, 1, 2, ..., 8. 9) contains a stimulus which is depicted by a red-colored dot. This stimulus or red-colored dot moves through a path on each corresponding digit. So, each digit forms a trajectory for the stimulus. A user has to follow the moving red stimulus of the corresponding digit in order to key in his or her PIN digits. PathWord is a touch-free gaze PIN entry method. Thus, shoulder surfers are not aware of the entered PIN digits using direct observation. The proposed method also provides a moderate resistance against video-based recording attacks. PathWord, however, is vulnerable to spyware-based recording attacks. The error rate and the required PIN-entry time of PathWord were evaluated via a user study of 42 participants. It is found that the percentage of error rate when entering a PIN digit using PathWord is high due to the limitation of eye detection. The required time for a user to enter his or her PIN digits is acceptable (about 6 seconds). The questionnaire results manifest that users prefer the regular PIN-entry method for everyday use rather than the PathWord because of its fast input.

J.-I. Lee et al. (2017) proposed a PIN-entry method named Reflector for mobile devices and desktop computers. Reflector uses an eye as a cursor to input the PIN password based on the private pointing on the reflected screen. The proposed method, i.e., Reflector, makes use of private pointing so as to stop observers or shoulder surfers who cannot watch the

same reflected virtual keypad image that the user watches on the screen. The experimental results guarantee the robustness of the proposed PIN-entry method (i.e., Reflector) for the distance change as compared with eye tracker PIN-entry methods. Even though Reflector reduces the effect of shoulder-surfing attack, it is still vulnerable to both video-based and spyware-based recording attacks.

EyeSec is an eye tracker PIN-entry method proposed by Li et al. (2017) in order to resist shoulder-surfing attacks. Look and dwell is the principle followed by this method to enter a PIN password. A user has to gaze at the desired PIN digit and dwell for a moment in order to perform authentication. It is found that EyeSec has a low success rate, and users take a long time to key in their PIN digits. Although EyeSec is resistant to shoulder-surfing and video-based recording attacks, it is prone to spyware-based recording attacks.

SafetyPIN is another gaze interaction PIN entry method introduced by (Seetharama et al., 2015) for securing ATM and POS systems using eye tracking. SafetyPIN is not really a look and shot method. A user needs to look and blink using his or her eyes instead of pressing a button (i.e., shot) in order to confirm the PIN entry. Eye blinking helps to avoid the observation attackers such as shoulder surfers who can gain information through the button pressing or keypad touching feedback. Weaver et al. (2011) proposed an analogous gaze-based PIN-entry method, EyeDent, so as to beat the practice of shoulder-surfing attacks. It clears the need for dwell time or physical feedback such as button pressing required to confirm the selection. EyeDent automatically clusters the gaze points to confirm the choice of a user's PIN digit. The experimental results of both methods, SafetyPIN and EyeDent, produced promising results in relation to PIN-entry time and error rate. For security, SafetyPIN and EyeDent can provide high and moderate resistance against shoulder-surfing and video-based recording attacks. However, they are prone to the threat of spyware-based recording attacks.

Almost all of the gaze-based methods are highly resistant to shoulder-surfing attacks, as observers generally experience difficulty catching the PIN when it is entered using their eyes. These PIN-entry methods are highly resistant to shoulder-surfing attacks. They may further reduce the threat of video-based recording attacks. All reported results showed that gaze-based methods are partially resistant when recording a user's gaze input and touch input multiple times (Binbeshr et al., 2020). However, they are susceptible to spyware-based recording attacks because users still reveal the original PIN during the authentication process. Furthermore, the application of gaze interaction methods is too limited because these methods fail to meet high accuracy, cost, and user experience requirements (Li et al., 2017). Table 2.1 presents a summary of the gaze-based PIN-entry methods resistant to Shoulder-Surfing Attack (SSA) as well as recording attacks (video-based and spyware-based).

2.4.1.2 Visual Distraction Methods

The visual distraction methods endeavor to distract observers visually instead of the indirect input of the PIN. They are classified into cursor camouflage, input distraction, and keypad distraction.

(a) ***Cursor Camouflage***

Cursor camouflage methods (Still & Bell, 2018; Sugumar & Soundararajan, 2017; Watanabe et al., 2012) typically mask the real cursor in order to distract the observer. For instance, Still and Bell (2018) proposed a cursor camouflage method named Incognito that hides the mouse cursor and transforms it into a border-selecting key when it passes over the keypad. The numeric keys vary from an active and inactive state to camouflage the one that represents the mouse cursor. The assessment results of Incognito show its capability to reduce the effect of shoulder-surfing attacks. Still, the Incognito PIN-entry method

Table 2.1: A summary of gaze-based PIN-entry methods

Author(s) & Year	Resistant to			Limitations
	SSA	Video	Spyware	
SM et al. (2021)	High	Moderate	Vulnerable	-High login time
Das et al. (2020)	N/A	N/A	N/A	-High login time
Carneiro et al. (2019)	High	Moderate	Vulnerable	-High login time
Ibrahim and Ambreen (2019)	Moderate	Low	Vulnerable	-Error rate not reported
Kumar et al. (2019)	High	Moderate	Vulnerable	-High error rate
Almoctar et al. (2018)	High	Moderate	Vulnerable	-High error rate
Holland and Morelli (2018)	High	Moderate	Vulnerable	-High login time -High error rate
Khamis et al. (2017)	High	Moderate	Vulnerable	-High login time -Error rate not reported
J.-I. Lee et al. (2017)	High	Moderate	Vulnerable	-Error rate not reported
Li et al. (2017)	High	Moderate	Vulnerable	-High login time -High error rate
Seetharama et al. (2015)	High	Moderate	Vulnerable	–
Weaver et al. (2011)	High	Moderate	Vulnerable	–

is susceptible to both video-based and spyware-based recording attacks. With respect to usability evaluation, Incognito is found more erroneous than the regular PIN-entry method. It is also not recommended by participants to replace the regular PIN method. The required PIN-entry time a user takes to login using the Incognito PIN-entry method was not reported.

Sugumar and Soundararajan (2017) and Watanabe et al. (2012) proposed cursor camouflage PIN-entry methods that typically mask the real cursor with dummy ones to distract the observer. The keys of the numeric keypad are randomly generated after each PIN digit entered by a user. Such methods may provide high resistance against shoulder-surfing attacks. However, they are prone to both recording attacks (video and spyware). The PIN-entry time a user needs to login using these methods is expected to be high due to the generation of a random numeric keypad for each PIN digit.

(b) ***Input Distraction***

In input distraction methods such as those Guerar et al. (2019) and P. Shi et al. (2009), a user is required to align his or her PIN digits together and submit all decoy digits to prevent the observer from obtaining the actual PIN. Such methods can reduce the success rate of shoulder-surfing attacks. For recording attacks (video-based and spyware-based), the adversary needs only to capture two recorded authentication sessions in order to recover the original PIN of a victim. An apparent limitation of P. Shi et al.'s method is the high login time required by a user to enter his or her PIN digits. With respect to the limit of Guerar et al.'s PIN-entry method, it is only designed for smartwatches.

An input distraction PIN-entry method named ForcePIN (Krombholz et al., 2016) uses a pressure-based mechanism where a user enters his or her PIN digits using a deep or shallow pressure in order to improve the PIN security by having higher PIN entropy or PIN space while maintaining an acceptable level of usability. Two user studies (lab and

field) were conducted to evaluate the performance of the ForecPIN PIN-entry method. The evaluation analysis concluded that ForecPIN maintains a low PIN-entry time and error rate when entering a PIN password. For security, ForecPIN can be defeated by shoulder-surfing and both video-based and spyware-based recording attacks.

Takada and Kokubun (2014) proposed a keypad distraction method that enables users to input multiple PIN digits simultaneously instead of the one-by-one input to disrupt observers. The proposed method is not secure against shoulder-surfing, video-based recording, and spyware-based recording attacks. The error rate was not reported by the study. A similar method was proposed by Leftheriotis (2013), where it lets people enter the PIN digits by tapping the right number of fingers on the multi-touch screen. This way of entering the PIN reduces the visibility in which it hides the fingers and breaks up the action. Although the proposed PIN-entry method could be immune to shoulder-surfing attacks, it is susceptible to video-based and spyware-based recording attacks. One significant problem of the study is that the proposed PIN-entry method was not evaluated.

(c) ***Keypad Distraction***

Keypad distraction methods, such as Adithya et al. (2017); Kabir et al. (2020); Nandhini and Jayanthy (2019) present a random digit keypad to frustrate a shoulder-surfing attacker. A user is presented with a random digit keypad layout whenever he or she wants to enter his or her PIN password. An obvious limitation of these methods is that they were not implemented and evaluated.

The other keypad distraction methods (Anthonio & Kam, 2020) and (Papadopoulos et al., 2017), blend two keypads so that a user who looks at the device from a close distance observes one keypad, while an attacker who looks at the device from a far distance observes the other keypad. These keypad distraction methods could not provide full resistance against shoulder-surfing attacks. In fact, the visibility is varied between users, and the

viewing distance of the attacker is not guaranteed to be equal to or bigger than the safety distance in real-world scenarios. The limitations of these proposed PIN-entry methods are as follows. A user may take a long time to enter his or her PIN password using Anthonio and Kam's method. Papadopoulos et al. (2017) did not evaluate their proposed PIN-entry method in terms of usability.

Overall, visual distraction methods can be used to protect against shoulder surfing attacks in a variety of ways. However, they are vulnerable to video-based or spyware-based recording attacks or both, because the attacker can get the original PIN from the recording tool no matter what the visual distraction tactics are. Table 2.2 summarises the visual distraction PIN-entry methods.

In a nutshell, the direct input PIN-entry methods try to distract the observer through gaze input or visual distraction. These methods may reduce the effect of the shoulder-surfing attacks. However, they are still susceptible to video-based recording spyware-based attacks (Tolosana et al., 2019). Thus, direct input methods are not taken into consideration in this research work.

2.4.2 Indirect Input Methods

The idea of indirect input methods is to prevent users from exposing the original PIN during each authentication attempt to thwart the adversary. Indirect input methods can be classified into challenge–response and others.

2.4.2.1 Challenge-Response Methods

The challenge-response approach is a typical example of indirect input methods in which a challenge is sent to the user through an audio, haptic, or visual channel. In particular, a user is given a challenge, and he or she needs to find out and input the response based on the received challenge and the original PIN. As a result, the user enters a one-time response per

Table 2.2: A summary of visual distraction PIN-entry methods

Author(s) & Year	Visual distraction method	Resistant to			Limitations
		SSA	Video	Spyware	
Kabir et al. (2020)	Keypad distraction	Low	Vulnerable	Vulnerable	-Usability was not evaluated
Anthonio and Kam (2020)	Keypad distraction	Moderate	Vulnerable	Vulnerable	-High login time
Guerar et al. (2019)	Input distraction	High	Low	Low	-Method designed for smartwatches
Nandhini and Jayanthy (2019)	Keypad distraction	Moderate	Vulnerable	Vulnerable	-Method was not evaluated
Still and Bell (2018)	cursor camouflage	Moderate	Vulnerable	Vulnerable	- Login time not reported
Adithya et al. (2017)	Keypad distraction	Moderate	Vulnerable	Vulnerable	-Method was not evaluated
Papadopoulos et al. (2017)	Keypad distraction	Moderate	Vulnerable	Vulnerable	-Usability was not evaluated
Sugumar and Soundararajan (2017)	cursor camouflage	High	Vulnerable	Vulnerable	-Method was not evaluated -Login time expected to be high
Krombholz et al. (2016)	Input distraction	Vulnerable	Vulnerable	Vulnerable	-Not secure
Takada and Kokubun (2014)	Input distraction	Vulnerable	Vulnerable	Vulnerable	-Not secure -Error rate was not reported
Leftheriotis (2013)	Input distraction	Moderate	Vulnerable	Vulnerable	-Method was not evaluated
Watanabe et al. (2012)	cursor camouflage	High	Vulnerable	Vulnerable	-Method was not evaluated
P. Shi et al. (2009)	Input distraction	Moderate	Low	Low	-High login time

session to reduce the threat of shoulder-surfing and recording attacks. Challenge-response methods are divided into audio-based, haptic-based, and visual-based based on how the challenge is sent, and how the response is given.

(a) ***Audio-Based Methods***

Several studies (Dan & Ku, 2017; Hirakawa et al., 2015, 2017; Jeon & Yoon, 2015; M.-K. Lee, Nam, & Kim, 2016; Perković, Čagalj, & Rakić, 2010; Perković, Čagalj, & Saxena, 2010; Rajarajan et al., 2018; Seo & Kim, 2017) have employed audio-based challenge-response methods to defend against shoulder-surfing, video-based recording, and spyware-based recording attacks. In audio-based methods, the challenge is sent through an audio channel. The user then needs to provide the response based on the received challenge and the original PIN.

SpinPad (Rajarajan et al., 2018) is an audio-based challenge-response aimed to strengthen the security of the entered PINs against shoulder-surfing and recording attacks. A user receives a random token (an alphabet) through the headphone, and then he or she aligns this alphabet token with the first PIN digit on a rotary interface. The user repeats the same process when entering the other PIN digit. SpinPad sends a random alphabet token per each PIN digit entry via the audio channel (i.e., the headphone). The security of the SpinPad method was tested using a security analysis, and a user study was conducted to evaluate the SpinPad's usability. It is found that SpinPad is immune to shoulder-surfing, video-based, and spyware-based recording attacks. With regard to the usability performance, SpinPad requires high login time due to the multiple round input of the PIN digits, in addition to the delay required to receive the challenge through the voice channel. SpinPad has some shortcomings. The audio channel is assumed to be secure. The error rate was not reported by the conducted user study. Furthermore, SpinPad requires an audio channel of communication which contradicts PIN's desirable requirement of being easy and fast.

Dan and Ku (2017) proposed an audio-based challenge-response PIN method, called Audi-PES, in order to resist shoulder-surfing and recording attacks, without the use of an earphone. Audi-PES works by covertly conveying the challenge at low volume. That is, a user needs to put the phone on his or her ear to hear the challenge. He or she needs to press the volume button so as to enter the response. The proposed PIN-entry method is capable of resisting shoulder-surfing and video-based attacks. It is also capable of defeating spyware attacks as long as the audio channel is secure. Nonetheless, there are some limitations to the proposed PIN-entry method. The average PIN-entry time is high (17 seconds). User satisfaction should be tested to know their willingness to put a phone on their ears around for 17 seconds to enter the PIN.

An audio-based challenge-response authentication method was introduced by Hirakawa et al. (2017) in order to secure the PIN entry against shoulder-surfing and recording attacks. The proposed PIN-entry method provides an interface (display icons) and sounds that are independent of any language (sound of animals, sound of instrumental tools). To input your PIN password using this audio-based PIN-entry method, you need to align a PIN digit to the location of the heard challenge using a rotary interface. To illustrate, you may align your PIN digit to the location of the corresponding icon of the heard challenge (e.g., a cat voice and its corresponding icon on the rotary interface). The proposed PIN-entry method is assumed to have a secure audio channel of communication. Thus, It is supposed to be resistant to shoulder-surfing and both video-based and spyware-based recording attacks, in spite of the absence of the security evaluation. Users may take a longer time to enter their PIN passwords using the proposed method because it requires multiple rounds to enter the PIN digits.

A bimodal (visual and audio) PIN-entry method was proposed by Seo and Kim (2017) so as to hide the secret information (i.e., PIN password) that is delivered during the

authentication process. The proposed PIN-entry method makes use of an audio channel to transmit a hint or an indicator of a challenge. A user maps his or her target digit of the PIN over an alphabet keypad based on the transmitted indicator. The indicator is a letter that represents the value zero ('0'). The user counts based on the PIN digit in a circular form and confirms the right letter to enter as part of the response. The user needs to repeat this process for each PIN digit. The proposed PIN-entry method provides low resistance against shoulder-surfing, video-based recording, and spyware-based recording attacks. The usability performance of the proposed PIN-entry method could be hindered due to the need for an earphone to convey the challenge and the requirement of multiple rounds to enter the PIN digits.

An analogous audio-based challenge-response PIN-entry method to Seo and Kim is the one that was proposed by M.-K. Lee, Nam, and Kim (2016). It is a bimodal method (visual and audio) where part of the challenge is vocalised via an audio channel and is mapped to a visual challenge to identify the response. That is, a user recognises the position of the vocalised challenge (alphabet) and moves it to the position of a PIN digits. The user repeats this process for all PIN digit. The proposed PIN-entry method is resistant to shoulder-surfing as well as recording attacks (both video-based and spyware-based). The average PIN-entry time for a user to enter his or her PIN is relatively high. One limitation of such a method is the requirement of a headphone in order to proceed with the authentication process. Users may feel uncomfortable preparing it whenever they enter their PIN passwords. Another concern of this proposed method is the requirement of multiple rounds a user needs to enter his or her PIN digits.

Hirakawa et al. (2015) proposed a voice-based PIN authentication method in order to tolerate shoulder-surfing and video-based recording attacks. The proposed PIN-entry method employs voice guidance to move a PIN digit to the correct place on a rotary interface.

This process should be repeated by a user for all PIN digits. The proposed PIN-entry method can provide high tolerance against shoulder-surfing, Video-based recording, and spyware-based recording attacks because of hiding both the challenge and PIN digits. In the evaluation test, the average authentication time the participants took to enter their PIN digits was about 22 seconds. The users took a long time to enter their PIN passwords using the proposed method because they needed to listen to the voice guidance and then move each PIN digit to the correct place. These multiple rounds of entering the PIN digits may have implications on the proposed method's usability.

Jeon and Yoon (2015) proposed a non-visual audio-based PIN authentication method for ATM, mobile lock, and electronic doors. The proposed method is called the Simple PIN Input Technique (SPIT). SPIT is aimed to countermeasure the practice of shoulder-surfing and recording attacks by employing sound cues to help a user to input his or her PIN. Initially, the SPIT system prepares a randomised list of 10 digits (0, 1, 2, ..., 8, 9). Then, the first digit (i.e., sound cue) of the list is vocalised. The user needs an earphone to receive the sound cue. He or she confirms his or her input when the received sound cue corresponds to a PIN digit. SPIT can provide high resistance against shoulder-surfing, video-based recording, and spyware-based recording attacks. However, it requires multiple rounds in order to key in a PIN password. With respect to usability performance, the SPIT method was not evaluated in terms of PIN-entry time and error rate.

An audio channel challenge-response PIN-entry method - Mod10-table - was proposed by Perković, Čagalj, and Saxena (2010) in order to resist shoulder-surfing and recording attacks. The proposed method relies on a mod 10 addition lookup table to assist users in entering their PIN passwords. The idea of this method is that a user employs his or her PIN and the received challenge to apply a simple lookup on the Mod 10 addition table to identify the response. The challenge is assumed to be sent through a secure audio

channel (e.g., earphones). The proposed method could be resilient against shoulder-surfing, video-based recording, and spyware-based recording attacks. In addition, it requires a reasonably PIN-entry time for a user to log in. However, the proposed PIN-entry method suffers from some limitations. For instance, it exhibits a high error rate (16%) when a user enters his or her PIN password. The requirement of multiple rounds for a user to key in his or her PIN password is another limitation of this proposed PIN-entry method.

Perković, Čagalj, and Rakić (2010) proposed a challenge-response PIN-entry authentication method - Shoulder Surfing Safe Login (SSSL) - in order to secure the PIN entry process in the presence of shoulder surfers and other recording attackers. There are three main components of the SSSL method: the secure channel, the SSSL table, and the input buttons. The secure channel is an audio channel that is occupied by SSSL to send the challenge (e.g., earphones). The SSSL table includes the digits 1,2,3, ..., 8, and 9. The digits are organised in a way that each digit is immediately adjacent to the other eight digits. The input buttons are the north west arrow, upwards arrow, north east arrow, leftwards arrow, circle, rightwards arrow, south west arrow, downwards arrow, and south east arrow. A user responds by clicking the buttons that represent the relative position of the challenge with respect to the PIN digits based on the SSSL table. SSSL is immune to shoulder-surfing, video-based recording, and spyware-based recording attacks while it ensures a secure audio channel to transfer the challenge. It is also important to mention that the required PIN-entry time a user needs to enter his or her PIN password using SSSL is relatively low (less than 10 seconds). Nonetheless, the requirement of multiple rounds for entering a PIN password might have serious implications for the usability of the SSSL PIN-entry authentication method.

These audio-based PIN-entry methods can provide high resistance against shoulder-surfing, video-based recording, and spyware-based recording attacks as long as the channel

that transfers the challenge is secure. In particular, all of these methods assume the audio channel, which transfers or receives the challenge, is secure. Still, this is an assumption, and it is better to send the response through this secured channel instead of the hassle of the challenge-response approach. Most importantly, these audio-based challenge-response PIN authentication methods require an additional channel (i.e., audio) in addition to the visual one that is used to enter the response. However, requiring an extra channel may make people less likely to accept and use these methods because it doesn't meet the compatibility condition of the PIN-entry method (Nyang et al., 2018). A summary table of the audio-based challenge-response PIN-entry method is shown in Table 2.3.

(b) ***Haptic-Based Methods***

Haptic-based challenge-response methods (Chakraborty et al., 2016; Higashiyama et al., 2015; Ku & Xu, 2019; Kwon & Hong, 2015; Luo et al., 2020; Souza et al., 2018; Uellenbeck et al., 2015; Xu et al., 2016) make use of a haptic channel in order to receive the challenge. The user then needs to provide the response based on the received challenge and the original PIN. For example, Luo et al. (2020) proposed a haptic-based challenge-response PIN-entry method for mobile authentication in order to prevent the threat of shoulder-surfing, video-based recording, and spyware-based recording attacks. The proposed method employs the device vibration to receive the challenge. In other words, it uses the device vibration to encode the challenge using the dot (.) and the dash (-). The dot symbolises the short vibration, and the dash symbolises the long vibration. Each digit has a vibration code or pattern. Three variations of the proposed method were designed regarding the way of delivering the challenge to the user. These variations are: Hint and Wait (HaW), Hint and calculate (HaC), and Calculate or Not (CoN). The challange (i.e., vibration) in HaW represents a position; it represents a number in HaC; it represents a sign in CoN. The user needs to identify the challenge and know the original PIN in order to

Table 2.3: A summary of audio-based challenge-response PIN-entry methods

Author(s)	Resistant to			Limitations
	SSA	Video	Spyware	
Rajarajan et al. (2018)	High	High	High	-Assumed a secure channel -Requires an additional channel -High login time -Error rate not reported
Dan and Ku (2017)	High	High	High	-Assumed a secure channel -Requires an additional channel -High login time -Error rate not reported
Hirakawa et al. (2017)	High	High	High	-Assumed a secure channel -Requires an additional channel -High login time -Requires multiple rounds
Seo and Kim (2017)	Low	Low	Low	-Assumed a secure channel -Requires an additional channel -Error rate not reported -Requires multiple rounds
M.-K. Lee, Nam, and Kim (2016)	High	High	High	-Assumed a secure channel -Requires an additional channel -High login time -Requires multiple rounds
Hirakawa et al. (2015)	High	High	High	-Assumed a secure channel -Requires an additional channel -High login time -Requires multiple rounds -Requires voice guidance
Jeon and Yoon (2015)	High	High	High	-Assumed a secure channel -Requires an additional channel -login time not reported -Error rate not reported -Required multiple rounds
Perković, Čagalj, and Saxena (2010)	High	High	High	-Assumed a secure channel -Requires an additional channel -High Error rate -Requires multiple rounds
Perković, Čagalj, and Rakić (2010)	High	High	High	-Assumed a secure channel -Requires an additional channel -Requires multiple rounds

produce the response. The proposed PIN-entry method can resist the attacks resulting from shoulder-surfing and video-based recording. However, it is vulnerable to spyware-based recording attacks. With respect to usability performance, the assessment results manifest that all variations of the proposed method have relatively high PIN-entry times with a high error rate.

A PIN-entry method - VpointsPES - was proposed by Ku and Xu (2019) in order to withstand shoulder-surfing attacks using localised haptic feedback. VpointsPES is a challenge-response PIN-entry method in which a user receives the challenge (feels the vibration pattern) through a localised haptic feedback, and then he or she aligns the challenge (letter) slot with the PIN digit slot on the response window. The proposed PIN-entry method has three configuration modes according to the partitions of the login rounds: low security and high efficiency (two login rounds), moderate security and moderate efficiency (three login rounds), and high security and low efficiency (four login rounds). Even though the VpointsPES PIN-entry method can withstand shoulder-surfing attacks, it can be broken through two recorded authentication sessions using video-based recording or spyware-based recording attacks. In spite of the high success rate, the usability user study reveals that the average PIN-entry time of the proposed PIN-entry method is relatively high for all modes (more than 10 seconds). Moreover, users are required to enter their PIN passwords through multiple rounds.

NomadicKey (Souza et al., 2018) is a challenge-response PIN-entry method that employs an out of band vibration channel in order to secure the PIN entry process. In the NomadicKey method, the positions of the keypad keys are randomly distributed to enhance security, whereas it keeps the same order of the regular keypad keys (i.e., 1, 2, 3, ..., 9,0) in order to maintain usability. All of these keyboard keys are highlighted during authentication, and randomly two of them are vibrated while being highlighted. A

user needs to identify these two keys and include them to the original PIN in any order and place during authentication. For example, suppose the user's PIN is 1234, and the vibrated keys are 89. To perform authentication, the user may enter any PIN password that includes his or her PIN digits and the vibrated keys in any order and place (e.g., 123489, 128934, 812394, etc.). The security analysis of the NomadicKey PIN-entry method shows that it can provide moderate resistance against shoulder-surfing attacks. However, Two recorded authentication sessions are required to break it using video-based recording and spyware-based recording attacks. The proposed PIN-entry method further is susceptible to accidental login attack. With regard to usability, the user spends a longer time to enter his or her PIN password using NomadicKey. This longer time results from the waiting time required to highlight all Nomadic keyboard keys.

An analogous haptic-based PIN-entry method to VpointsPES, named Loc-HapPIN, was proposed by Xu et al. (2016) in order to enhance the resistance to shoulder-surfing and recording attacks. Loc-HapPIN is a challenge-response approach in which the challenge is sent or received through the localised haptic feedback technology. To illustrate, a user gets the challenge by putting his or her five fingers on a haptic sensation region. Only one of the five points will randomly vibrate in order to represent the challenge. The user then aligns the PIN digits slots to the received challenge slot on a responsive User Interface (UI). The user requires multiple rounds in order to enter the response. The original PIN password is not entered. The Loc-HapPIN method can enhance the resistance to the shoulder-surfing attack. However, the adversaries who succeed in recording two authentication sessions using a video camera or spyware software can recover the original PINs of the victims. The usability performance of the proposed method was not well analysed and discussed.

Chakraborty et al. (2016) proposed a vibration signals PIN-entry authentication method in order to avoid the threat of shoulder-surfing and recording attacks. The proposed

resembles the SSSL challenge-response method (Perković, Čagalj, & Rakić, 2010) where a secure channel, the SSSL table, and input response buttons are used for authentication. The only difference is the secure channel; the proposed method employs a haptic channel instead of the audio channel used by the SSSL method. That is, the challenge is represented as a vibration stimulus by the proposed method. Four vibration sensors (Right, Left, Up, and Down) were used to simulate all input response directions (north west arrow, upwards arrow, north east arrow, leftwards arrow, circle, rightwards arrow, south west arrow, downwards arrow, and south east arrow). A user makes use of the localised haptic feedback in order to identify the direction, and hence he or she can provide the response. The security analysis of the proposed PIN-entry method confirms its effectiveness in resisting shoulder-surfing attacks as well as both recording attacks (video-based and spyware-based). The significant overhead of the login time and error rate are the main usability drawbacks associated with the proposed PIN-entry method.

A haptic-based PIN-entry method was proposed by Higashiyama et al. (2015) in order to combat shoulder-surfing and recording attacks. It is a challenge-response method where it focuses especially on the use of the device vibration to receive a challenge, and schemes such as digit addition to input a response. To receive a challenge, a user touches or moves the cursor over keypad keys to identify the challenge. One out of three vibration patterns is accompanied by each key of the keypad: the dot (.), the double dots (..), and the dash (-). The dot and double dots symbolise a single short vibration and two short vibrations, respectively. The dash represents a single long vibration. To input the response, the user makes use of the digit addition in which he or she adds the PIN digit to the challenge digit to form the response. If the addition result is above 10, the user should select the least significant digit (e.g., the digit 7 should be selected when the challenge and PIN digits are 9 and, respectively). The proposed PIN-entry method can reduce the threat of

shoulder-surfing attacks. However, it provides low resistance to video-based recording and spyware-based recording attacks because the adversary only needs two captured authentication sessions in order to recover the original PIN digits. The average PIN-entry time and error rate of the proposed method is less than 10 seconds and 10%, respectively.

Of the haptic-based challenge-response PIN-entry methods, Kwon and Hong (2015) proposed an improved version to the visual-based cognitive trapdoor game PIN-entry method (Roth et al., 2004), named TictocPIN. In the cognitive trapdoor game method, a user is asked to enter the background or aligned colours of the keypad digit keys instead of the 4/6-numeric PIN in order to disguise user input. Black and white are the only colours employed by this method. TictocPIN was mainly proposed to overcome the susceptibility problem of the cognitive trapdoor game method to recording attacks, in addition to some usability limitations such as round redundancy and high error rate. TictocPIN is different from the cognitive trapdoor game method in the way that it utilises a haptic channel to send or receive the challenge instead of the visual one. It also utlises four different coluors (black, white, red, and blue) instead of the black and white colours. There are two rounds to enter a PIN digit using TictocPIN; two different coluors are assigned to each keypad digit key in the first round; three different coluors are assigned to each keypad digit key in the second round. The user identifies the coluor of the digit key (i.e., response) that is associated with the vibration. The TictocPIN PIN-entry method provides high resilience to shoulder-surfing and recording attacks (video-based and spyware-based) as long as the haptic channel is secure. An apparent limitation of the proposed method is the significant slowness of entering a PIN password, i.e., a user needs an average of 15 seconds to complete the PIN entry process.

Uellenbeck et al. (2015) introduced a challenge-response PIN-entry method resistant to shoulder-surfing and recording attacks - TACO - using localised tactile feedback of a

device. To perform authentication, a user needs to hold the device and press the login button. Then, the TACO method outputs a pseudorandom number of vibration signals. The user counts these signals, adds their number to the current digit of his or her PIN, and inputs the resulting digit. If the addition result is above 9, the user need to provide the least significant digit (if the result is 19, the user should input 9). The same process is repeated for each digit of the user's PIN password. The proposed PIN-entry method is considered secure against should-surfing, video-based recording, and spyware-based recording attacks as long as the haptic channel (i.e., vibrations) used to pass the challenge is not accessed by the adversaries. For usability, the TACO method presents some limitations. The conducted user study demonstrates that the average PIN-entry time a user needs to input his or her PIN password is significantly high (about 36 seconds). This high PIN-entry time is attributed to the required time for vibrations and pauses, in addition to the calculation and response time.

Some haptic-based challenge-response PIN-entry methods can provide high resistance against shoulder-surfing, video-recording, and spyware attacks. However, these methods assume a secure channel to receive the challenge. Moreover, the requirement of the additional channel of communication (i.e., haptic) contradicts the compatibility condition of the PIN-entry method (Nyang et al., 2018). Table 2.4 provides a summary of the haptic-based challenge-response PIN-entry methods.

In a nutshell, the majority of the challenge-response PIN-entry methods take delivery of the challenge through a visual channel (Binbeshr et al., 2020). Audio-based and haptic-based methods are bimodal types that require a visual channel to input the response in addition to the challenge-receiving channel (audio or haptic). This condition gives preference to unimodal visual-based methods because the same channel is used to receive the challenge and input the response. Thus, this research work focuses on visual-based

Table 2.4: A summary of haptic-based challenge-response PIN-entry methods

Author(s)	Resistant to			Limitations
	SSA	Video	Spyware	
Luo et al. (2020)	Moderate	Moderate	Vulnerable	-Assumed a secure channel -Requires an additional channel -High login time -High Error rate
Ku and Xu (2019)	High	Low	Low	-Assumed a secure channel -Requires an additional channel -High login time -Requires multiple rounds
Souza et al. (2018)	Moderate	Low	Low	-Assumed a secure channel -Requires an additional channel -High login time -Error rate not reported
Xu et al. (2016)	High	Low	Low	-Assumed a secure channel -Requires an additional channel -Login time not reported -Error rate not reported -Requires multiple rounds
Chakraborty et al. (2016)	High	High	High	-Assumed a secure channel -Requires an additional channel -High login time -High Error rate
Higashiyama et al. (2015)	Moderate	Low	Low	-Assumed a secure channel -Requires an additional channel
Kwon and Hong (2015)	High	High	High	-Assumed a secure channel -Requires an additional channel -High login time
Uellenbeck et al. (2015)	High	High	High	-Assumed a secure channel -Requires an additional channel -High login time -Error rate not reported -Requires multiple rounds -Requires calculation

challenge-response methods. The details of the visual-based challenge-response PIN-entry methods are presented in the related work section.

2.4.2.2 Other Indirect Input Methods

Apart from the challenge-response methods, Dhandapani et al. (2021) proposed an indirect input PIN-entry method in which a user enters his or her PIN through swipes and tab gestures for discreet PIN-entry. The proposed PIN-entry method makes use of the Morse Code Vibration pattern in order to provide a feedback when a user interacts with the system. The user either swipes up to increase the current digit or swipes down to decrease the current digit. The selection is confirmed when the user tabs two times. Even though the proposed PIN authentication method succeeded in reducing the effect of shoulder-surfing attacks, it is still prone to video-based and spyware-based recording attacks. Moreover, the required PIN-entry time is high as compared with the regular PIN entry method. The other indirect input method (Alsuhibany & Almutairi, 2016) involves adding other decoy digits when entering the original PIN to resist the effect of shoulder-surfing attacks. The proposed method uses master key alongside the PIN to disguise attackers from getting the actual PIN. The master key is composed of two digits, an activator and deactivator. The actual PIN is entered after typing the activator. Digits after the deactivator and before the activator are considered camouflage digits. This indirect input method can provide a moderate resistance against the shoulder-surfing attack. However, it is vulnerable to recording attacks (video-based and spyware-based) where the attacker could get the original PIN by watching two recorded sessions and then getting the PIN from the first one. The usability performance of the proposed PIN-entry method was assessed through a questionnaire. However, the PIN-entry time and PIN-entry success rate were not reported.

2.5 Related Work

Visual-based challenge-response is a unimodal method in which the same visual channel is used to transfer the challenge and deliver the response. Thus, this could give such a method more preference than bimodal challenge-response methods (i.e., audio-based and haptic-based). For example, visual-based challenge-response methods have been proposed by Chakraborty et al. (2019), Kasat and Bhadade (2018), and Kwon et al. (2014) to resist shoulder-surfing attacks. These PIN-entry methods are similar to the cognitive trapdoor game method (Roth et al., 2004), in which users are asked to enter the background or aligned colours instead of the 4/6-numeric PIN in order to disguise user input. However, the proposed methods do not mitigate video-based or spyware-based recording attacks. More precisely, the attacker can easily narrow down the possible PINs by analysing the recorded authentication sessions. With regard to usability, these proposed PIN-entry methods may hamper usability by requiring multiple rounds to input PIN digits. Furthermore, it may be difficult to use such PIN-entry methods because they require a lot of time to input PIN digits.

Caporusso (2021) introduced a visual-based challenge-response PIN-entry method to defend against shoulder-surfing attacks. The proposed method makes use of a user-defined confirmation code utilised during the authentication process. The challenge is sent to the user as a random sequence of digits. To perform the authentication, a user presses the confirmation code (e.g., 5) when the current digit of the challenge matches the PIN digit. The proposed method conceals the PIN digits by entering the confirmation code in order to mitigate shoulder-surfing attacks. Although the proposed PIN-entry method could resist shoulder-surfing attacks, it is vulnerable to both video-based and spyware-based recording attacks. For usability, the user needs a long time to enter his or her PIN password using the proposed method, with relatively high error rate. Moreover, the proposed PIN-entry

method requires multiple rounds to perform the authentication.

AlignPIN (Jain et al., 2021) is a challenge-response indirect input PIN method, which employs the same visual channel, in order to resist repeated shoulder-surfing attacks. The basic idea of the AlignPIN method is to align each challenge digit with each PIN digit on a random 4x10 grid of cells in order to obscure the PIN entry process. Each grid cell has 4 digits: one leading digit and three random digits. Each row has all leading digits (0, 1, 2, ..., 8, 9), and they appear only one time with each row. A user needs to register a reference cell (row, column) during the registration phase so as to be used to identify the challenge digits during the login phase. The user needs to align each PIN digit with each challenge digit in each row of the random 4x10 grid of cells in order to perform authentication. AlignPIN provides high resistance against shoulder-surfing attacks. Indeed, it is difficult for shoulder surfers to remember all grid cells and the moving vectors entered by a user. However, it is still prone to video-based and spyware-based recording attacks where an attacker can recover the original PIN through two recorded sessions. Actually, the attack can identify the challenge grid cell within two recorded authentication sessions, and thus he or she can reproduce the original PIN password with the help of the recorded moving vectors entered by the user. A user study was conducted to analyse the usability of the proposed PIN-entry method according to the PIN-entry time and error rate. Two group users were recruited: young and old. The average PIN-entry time for both groups is significantly high (about 20 seconds for young users and about 33 seconds for old users). With respect to error rate, the experimental results shows that young users can enter their PIN passwords with low error rate (about 3%). The results show a higher error rate for old users (above 10%). AlignPIN is not compatible with the way you usually enter your PIN because of how the interface looks and what you remember. Moreover, the long PIN-entry time may hinder its adoption as an alternative to the regular PIN-entry method.

A physical protection challenge-response method named TTU was proposed by Nyang et al. (2018) to secure the PIN entry against recording attacks. A user needs to press two buttons using his or her thumbs to see the challenge and identify the response based on the challenge and the original PIN. It can be seen that TTU is moderately resistant to both shoulder-surfing and video-based recording attacks. Indeed, this method relies on the physical hand protection of the challenge. Therefore, improper user posture of the mechanism can reveal the PIN. TTU is vulnerable to spyware-based recording attacks because this type of attack cannot be defeated by physical protection. There are several limitations of the TTU method with respect to usability. The average PIN-entry time required by the user to enter his or her PIN digits is relatively high. likewise, the error rate of entering a PIN password is relatively high. Considering the design of the TTU method, it is limited to smart phone devices.

DynamicPIN was developed by J.-H. Kim et al. (2017) to secure ATM authentication from shoulder-surfing attacks. To thwart the attack, it uses a PIN, a secret number such as SSN or phone, and arithmetic operations to generate an OTP. The security analysis of the DynamicPIN authentication method reveals that it can only provide low resistance against shoulder-surfing and video-based and spyware-based recording attacks. This is actually because the adversaries just need two captured authentication sessions in order to reproduce the original PIN digits. The usability performance of the DynamicPIN method was tested using a user study in terms of login time and error rate (i.e., success rate). The assessment results showed that the average login time a user needs to key in is about 11 seconds, with a success rate of about 90%. One limitation of the proposed method, however, is that it requires human computation in order to produce the OTP. Another limitation in the DynamicPIN method involve the overhead of memorising more information other than the PIN password.

Seo et al. (2017) proposed a visual channel challenge-response PIN-entry method resistant to shoulder-surfing attacks for augmented reality devices such as google glass. The challenge is delivered through the augmented reality device (i.e., a small overlay screen), which is practically supposed to be a secure medium against shoulder surfers. The proposed PIN-entry method masks the PIN password by delivering offset numbers so as to obscure the PIN entry process. To perform authentication, a random number (i.e., challenge) is displayed on the small built-in screen of the augmented device (e.g., google glass). A user needs to enter the correct value (using the mobile device) that matches the original PIN password when added to the random number using module 10. For example, let the random number be 1123, and the user's PIN password is 2244. The correct value or response that should be entered by the user to be authenticated is 1121. A prototype of the proposed PIN-entry method was implemented in order to test its performance with respect to security and usability. The security analysis of the proposed PIN-entry method revealed that it is highly secure against shoulder-surfing attacks and video-based due to the employment of the small overlay screen to deliver the challenge. The security of the proposed PIN-entry method against spyware-based can be broken if the screen content of both devices is recorded. Regarding usability, the reported PIN-entry time was about 6 seconds, with a 100% PIN entry success rate. The proposed PIN-entry method presents some limitations. The PIN entry process relies on the augmented reality device, which contradicts the usability requirement of the PIN-entry method of adding an additional channel or device of communication (i.e., a visual channel). Another limitation of this method is its restriction to the augmented reality applications.

M.-K. Lee, Kim, and Franklin (2016) and M. Lee and Nam (2013) developed secured solutions to the regular PIN using a 3D display. The reason for employing the 3D display is to disguise the vision of the depth of the prominent digit or challenge digit. The prominence

of the prominent digit is different from the other decoy digits. So, a user who is at the 3D spot can only identify the prominent digit. This prominent digit is used together with the PIN digits to find out the response. 3DPIN is the name of the PIN-entry method proposed by M.-K. Lee, Kim, and Franklin (2016). It is similar to the traditional dial lock, where a user rotates a scroll wheel in order to enter a PIN. In the 3DPIN PIN-entry method, the digit with prominent depth is used as a start point to rotate the wheel based on PIN digits. The name of the other PIN-entry method, which was proposed by M. Lee and Nam (2013), is Map-3D. It is composed of two phases: the challenge submission phase and the response entry phase. In the first stage, a 10 by 10 matrix of alphabets is given to the user as well as the column index from 0 to 9. Each column is a random permutation of 10 alphabet characters from A through K. One letter of the 100 letters has a depth of +1, whereas the others have a depth of -1. The user who is at the 3D spot only can recognise this letter (prominent letter). He or she identifies the letters corresponding to his or her PIN digit on the column where the prominent letter is located. These challenge-response methods (3DPIN and Map-3D) could resist shoulder-surfing attacks, but they are vulnerable to both video-based and spyware-based recording attacks. Regarding usability, the 3DPIN method requires a relatively high PIN-entry time in order to input the PIN password. This high login time is a result of the multiple rounds a user spends during the PIN entry process. The Map-3D PIN-entry method may have a compatibility issue in designing an interface layout that is different than the interface layout of the regular PIN-entry method.

In 2015, Von Zezschwitz et al. proposed an indirect input PIN-entry method named SwiPIN that assigns a simple random touch gesture to each digit on the keypad in order to resist the shoulder-surfing attack. These random gestures are UP, DOWN, RIGHT, LEFT, and TAB. A user needs to recognise and draw the gesture that is assigned to his or her PIN character. The authors have conducted a security and usability evaluation of

the SwiPIN. They first evaluated the three designs of the proposed PIN entry method. Then, the best design was compared with the regular PIN-entry method. Even though the evaluation results showed that SwiPIN performs fast regarding login time, it is susceptible to shoulder-surfing attacks. The conducted user studies confirm that shoulder surfers could break the proposed PIN-entry method and recover the original PIN within a few trials. In particular, an attacker needs to be able to figure out what are the gestures drawn by the user in order to break the PIN. The proposed PIN-entry method is undoubtedly vulnerable to recording attacks (video-based and spyware-based). Nonetheless, the SwiPIN PIN-entry method could be considered usable because the average PIN-entry time (3 seconds) is comparable to the PIN-entry time required by the regular PIN method, and its error rate is relatively low (3%). Thus, it can be argued that SwiPIN could be adopted as an alternative to the regular PIN-entry method in critical security scenarios.

Kwon and Na (2015) proposed a visual-based indirect input method named SteganoPIN to resist video-based recording attacks. SteganoPIN consists of two numeric keypads: random (permuted) and standard. The random keypad is used to derive the new OTP. It permutes the 10 numeric keys randomly for each session. However, this keypad is hidden by default, and it appears in a small circular touch area when a user puts a cupped hand on this circle. The standard keypad is used to key in the OTP. The user first locates the original PIN on the random keypad and then maps the key locations onto the standard keypad for OTP derivation. The user then enters the OTP on the standard keypad. The security analysis of the SteganoPIN method demonstrated that the use of OTP resists the shoulder-surfing attacks. It also ascertained that it is secure against video-based recording attacks if a user correctly uses the system. SteganoPIN, however, is vulnerable to spyware-based recording attacks. The usability performance of the proposed PIN-entry method was measured through the PIN-entry time and success rate. The results of the

conducted user study manifests that SteganoPIN guarantees relatively fast PIN-entry time and low error rate. In other words, the average PIN-entry time was 5.7 seconds, and the average error rate was about 2%. There are some limitations of the proposed PIN-entry method. The perumted keypad used to drive the OTP is too small. Users may find it difficult to catch the OTP easily. Moreover, a user need to a cupped hand posture in order to derive the OTP. Thus, the security of the SteganoPIN method relies on the user's usage of the system.

Kwon and Na (2014); Vijai and Joseph (2018) proposed visual-based challenge-response PIN-entry methods in order to overcome shoulder-surfing and recording attacks. The proposed PIN-entry methods employ the same idea as the SteganoPIN method. To illustrate, both proposed methods employ two keypads: the challenge keypad and the response keypad. To perform authentication, a user needs to map his or her actual PIN on the challenge keypad to get the OTP, and then he or she types the latter on the response keypad. The numeric keys of the challenge keypad are permuted randomly per each authentication session. Vijai and Joseph (2018) did not evaluate or report any results about their proposed PIN-entry method. On the contrary, Kwon and Na (2014) evaluated their proposed PIN-entry method - SwithPIN - through a user study. However, the conducted user study was only used to measure the PIN-entry time of the SwitchPIN method. The reported PIN-entry time was about 3.5 seconds. In spite of missing the security analysis of these PIN-entry methods, they are supposed to provide the same security the SteganoPIN method provides with respect to shoulder-surfing attack resistance. However, they are susceptible to video-based recording attacks as well as spyware-based recording attacks. Actually, these proposed methods do not hide or protect the challenge keypad as the SteganoPIN method does. So, their resistance to video-based recording attacks is different from the SteganoPIN method.

A visual-based challenge-response PIN-entry method was proposed by Yadav et al. (2015) in order to provide a secure mechanism against shoulder-surfing attacks. The proposed mechanism utilises the google glass screen as the PIN-entry method proposed by Seo et al. (2017). The proposed PIN-entry method provides a keypad with randomly assigned numeric keys per each authentication session. A user needs to use the forward and backward swipes and tap gestures in order to key in his or her PIN digits. To illustrate, the user navigates to the required numeric key (i.e., a PIN digit) using the forward or backward swipes, and then he or she selects that PIN digit using the tapping gesture. This process of entering a PIN password is varied from one authentication session to another. That is, the number of movements and the sequence of gestures will be different from time to time. Hence, the adversaries may face difficulties in order to deduct the original PIN. Even though the proposed PIN-entry method can effectively resist the threat of shoulder-surfing attacks, it is still prone to video-based and spyware-based recording attacks. A usability test of 30 participants was conducted to evaluate the proposed PIN-entry method in terms of login time and success rate. The usability performance test results show that the average login time of a user to input his or her PIN password is relatively login (more than 10 seconds). In terms of success rate, a user can enter his or her PIN password using the proposed PIN-entry method with a success rate of about 87% of the time. There are some drawbacks to the proposed PIN-entry method. One of these drawbacks is that it limits the use of PIN passwords with identical digits. Another major drawback of this method is the lack of usability. A significant source of lacking usability is due to the high login time and the high error rate when a users enter his or her PIN password. Moreover, the work of the proposed PIN-entry method is limited to google glass.

M.-K. Lee (2014) presented a challenge-response method where its layout comprises an array of digits (0-9) juxtaposed with an array of 10 objects. In the first round, a user

identifies a session decision key, which is the object aligned with the first digit of the PIN. For subsequent rounds, the user aligns the session decision key with each PIN digit. Quantitative security analysis was performed in order to evaluate the security performance of the proposed PIN-entry method in terms of shoulder-surfing and recording attacks' resistance. Although the developed method is effective against shoulder-surfing attacks, it is susceptible to video-based and spyware-based recording attacks. In particular, the adversary can recover the original PIN password with two recorded authentication sessions. To assess the usability of the proposed PIN-entry method, a user study of 24 participants was conducted. The conducted user study was used to collect the PIN-entry time and error rate of the participants' PIN entry processes. It is remarkable that the average PIN-entry time is relatively low, and the success rate of entering a PIN password is high. A questionnaire was performed to collect user feedback about the developed PIN-entry method. The participants perceived different opinions with respect to the usage of the proposed PIN-entry method in daily authentication. A usability limit of this developed PIN-entry method is the requirement of multiple rounds to enter the PIN password.

A visual-based challenge-response PIN-entry method was proposed by M.-K. Lee and Nam (2013) in order to defend against shoulder-surfing attacks effectively. The proposed method uses a random mapping between the PIN digits and the challenge characters in order to conceal the PIN-entry process. There are two phases of the proposed PIN-entry method: the challenge phase and the response phase. In the challenge phase, the user is given a challenge keypad that displays a random mapping between the PIN digits and challenge characters. That is, each digit in this keypad is associated with a challenge character. Challenge characters are given from the English alphabet (i.e., A, B, C, ..., x, Y, Z). In the response phase, the user is required to identify this mapping and then enter these mapped characters instead of the direct input of the original PIN digits. The proposed

PIN-entry method can combat shoulder surfers because it is difficult for them to memorise the instant map that lasts for a few seconds. However, it is vulnerable to video-based and spyware-based recording attacks. An experimental test was conducted to assess the usability performance of the proposed PIN-entry method in terms of PIN-entry time and error rate. The results of the experimental test manifest that the proposed PIN-entry method is relatively fast and accurate. Precisely, the average PIN-entry time a user takes to input his or her PIN digits password is about 6 seconds, with a success rate of about 93%.

Overall, many visual-based challenge-response methods resistant to shoulder-surfing and recording attacks have been proposed in the literature. These methods are preferred over the other challenge-response methods due to their compatibility with the regular PIN regarding the communication channel. However, the analysis of these PIN-entry methods shows their weaknesses in resisting recording attacks. A summary of these methods is presented in Table 2.6.

2.6 Chapter Summary

The literature review of PIN-entry methods resistant to shoulder-surfing and recroding attacks was discussed in this chapter. These methods are classified into direct and indirect PIN-entry methods. The direct PIN-entry methods try to disguise the observer through gaze-based and visual distraction methods. The visual distraction methods include cursor camouflage, input distraction, and keypad distraction methods. Even though direct input PIN-entry methods are capable of reducing the effect of shoulder-surfing attacks, they are still prone to recording attacks. The indirect input methods are categorised into challenge-response and others. The challenge-response methods include audio-based, haptic-based, and visual-based methods. Audio-based and haptic-based methods require additional channels of communication (i.e., audio and haptic) to convey the challenge. This gives the visual-based methods more preferences where the same visual channel is

Table 2.5: A summary of the related work PIN-entry methods

Author(s)	Method	Resistant to			Limitations
		SSA	Video	Spyware	
Caporusso (2021)	Entering a user-defined confirmation code instead of the PIN digits	Moderate	Vulnerable	Vulnerable	-High login time -High error rate
Jain et al. (2021)	Align each PIN digit with each challenge digit in each row of a random 4x10 grid of cells	High	Low	Low	-Not compatible interface layout -More memorized information -High login time
Chakraborty et al. (2019)	Input of the background color of the PIN digits	High	Vulnerable	Vulnerable	-Requires multiple rounds -High login time
Kasat and Bhadade (2018)	Input of the background color of the PIN digits	High	Vulnerable	Vulnerable	-Requires multiple rounds -login time not reported -Error rate not reported
Nyang et al. (2018)	Physical protection of the challenge area	Moderate	Moderate	Vulnerable	-High login time -High error rate -Limited to smart phones
Vijai and Joseph (2018)	two keypads - challenge and response	Moderate	Vulnerable	Vulnerable	-Similar to StegnoPIN method -Requires multiple rounds -login time not reported -Error rate not reported

continued on next page

Table 2.5: A summary of the related work PIN-entry methods (cont.)

Author(s)	Method	Resistant to			Limitations
		SSA	Video	Spyware	
J.-H. Kim et al. (2017)	OTP based on a PIN, secret no like SSN/phone and arithmetic operation	Low	Low	Low	-Requires human computation -More memorized information -High login time
(Seo et al., 2017)	a small overlay screen to deliver the challenge	High	High	vulnerable	-Requires a hardware device -restricted to augmented reality applications
M.-K. Lee, Kim, and Franklin (2016)	3D display to disguise the vision of challenge digit	Moderate	Vulnerable	Vulnerable	-High login time -Requires multiple rounds
Kwon and Na (2015)	Physical protection of the challenge area	Moderate	Moderate	Vulnerable	-Should be installed & used correctly -Requires proximity sensor -Designed for stationary systems
Von Zezschwitz et al. (2015)	Draw the gesture assigned to each PIN digit	Moderate	Vulnerable	Vulnerable	-Requires multiple rounds
Yadav et al. (2015)	Enter PIN digits using forward and backward swipes and tapping gestures	High	Vulnerable	Vulnerable	-Restricts the use of PIN passwords with identical digits -High login time -High error rate -limited to google glass

continued on next page

Table 2.5: A summary of the related work PIN-entry methods (cont.)

Author(s)	Method	Resistant to			Limitations
		SSA	Video	Spyware	
Kwon and Na (2014)	two keypads - challenge and response	Moderate	Vulnerable	Vulnerable	-Error rate not reported -Security was not evaluated
M.-K. Lee (2014)	Align the challenge digit to each PIN digit	Moderate	Low	Low	-Requires multiple rounds
Kwon et al. (2014)	Input of the background color of the PIN digits	High	Vulnerable	Vulnerable	-Similar to StegnoPIN method -Requires multiple rounds -login time not reported -Error rate not reported
M. Lee and Nam (2013)	3D display to disguise the vision of challenge digit	Moderate	Vulnerable	Vulnerable	–Not compatible interface layout
Leftheriotis (2013)	mapping between the PIN digits and alphabets given as challenges	Moderate	Vulnerable	Vulnerable	-Requires multiple rounds -login time not reported -Error rate not reported
Roth et al. (2004)	Input of the background color of the PIN digits	High	Vulnerable	Vulnerable	-Similar to StegnoPIN method -Requires multiple rounds -login time not reported -Error rate not reported

used for both receiving the challenge and entering the response. This research focuses on the visual-based challenge-response methods discussed in the related work section. Nonetheless, these visual-based indirect input methods provide no protection against video-based recording and spyware-based recording attacks. Therefore, the development of a secure and usable visual PIN-entry method against such attacks would be promising. The other indirect input PIN-entry methods are susceptible to recording attacks.

CHAPTER 3: RESEARCH METHODOLOGY

3.1 Introduction

This chapter describes the methodological approach undertaken to achieve the objectives of this research. A research methodology framework of four successive phases is adopted; each is described in a separate section. This chapter ends with a summary section.

3.2 Research Methodology Framework

The research methodology is broken down into four phases, as presented in Figure 3.1. These phases are systematic review, proposed PIN-entry method design, prototype implementation, and evaluation and analysis. Each of which is mapped to one of the research objectives mentioned in Chapter 1.

3.2.1 Phase1: Systematic Literature Review (SLR)

In the first phase, a SLR has been conducted on the existing PIN-entry methods that resist shoulder-surfing and recording attacks. The SLR is a formal way to identify, appraise, and synthesise all high quality research evidence based on eligibility criteria, to answer a research question(s) (Keele et al., 2007; Kofod-Petersen, 2012). The purpose of using a SLR is not limited to summarise the existing shreds of evidence of a research question, identify the gab, or highlight the future directions. It can also be undertaken to reduce the bias, resolve the conflict of evidences, and support the reporting guidance.

This phase is mapped to the first research objective of reviewing the existing PIN-entry methods resistant to shoulder-surfing and recording attacks. The conducted SLR comprises three stages: planning the review, conducting the search, and reporting the results. This SLR makes use of guidelines set by PRISMA (Hutton et al., 2015) in order to construct a review protocol and report the results of this SLR.

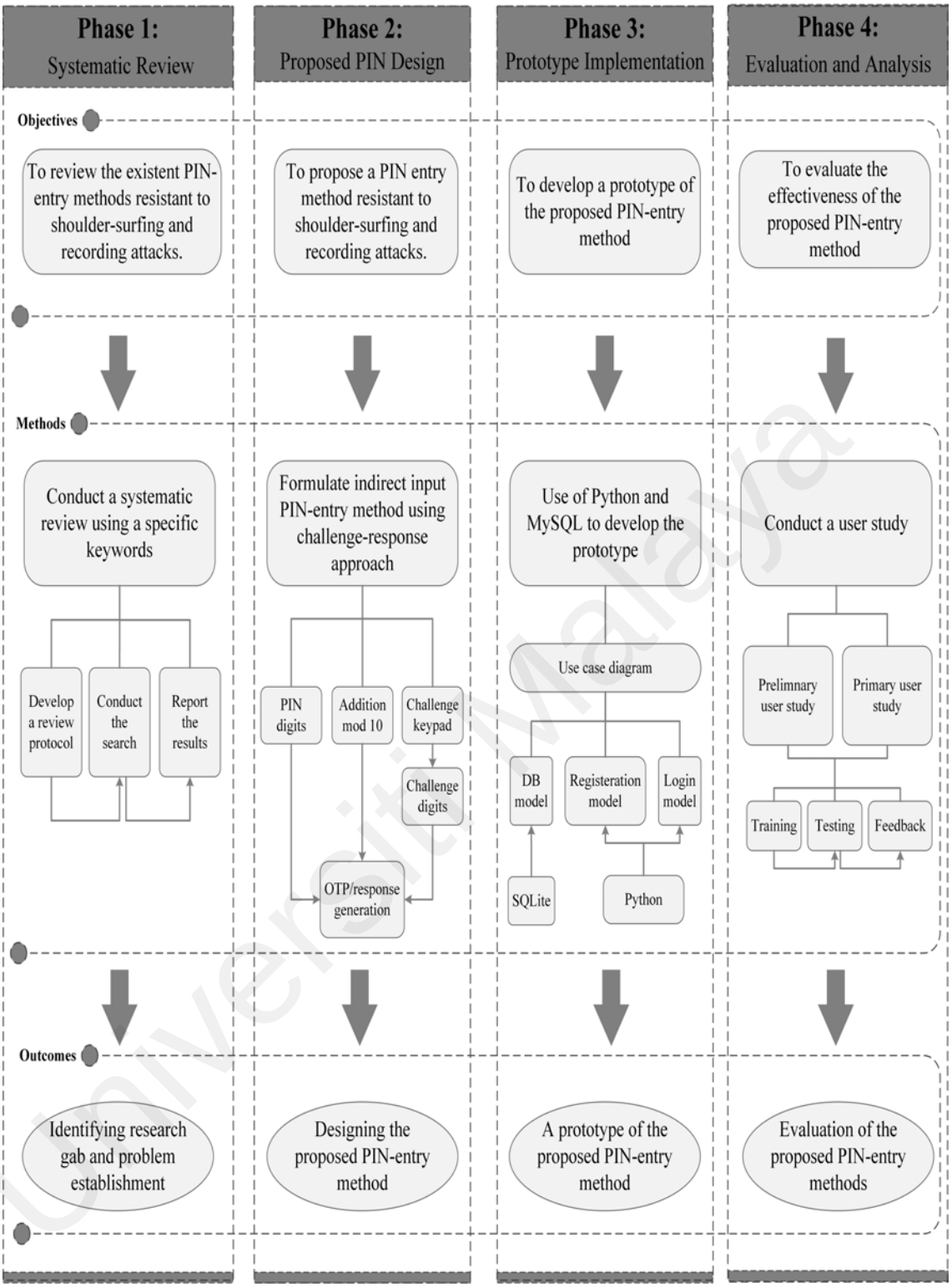


Figure 3.1: Research Methodology Framework

3.2.1.1 Planning Stage

The planning stage involves developing the review protocol of the SLR. The review protocol development includes research questions, eligibility criteria (i.e., inclusion and exclusion criteria), information sources, search strategy, quality assessment criteria, and

data extraction strategy. The review protocol has been approved by three people (i.e., the student and his supervisors).

(a) ***Research Questions***

The objective of this SLR is to review the existent PIN-entry authentication methods resistant to shoulder-surfing and recording attacks in order to identify the main challenges that impede their acceptance and adoption and provide a pledge to appropriately conduct further research activities. In order to meet this objective, the following research question and sub-questions have been developed:

What are the existent PIN-entry methods resistant to shoulder-surfing attack in the literature?

- What evaluation metrics were used to evaluate the PIN-entry methods?
- What are the limitations and open solutions/recommendations of the current PIN-entry methods?

(b) ***Eligibility criteria***

This SLR includes all the articles that meet the following inclusion criteria (IC):

IC1 Articles that deal only with PIN-entry authentication methods resistant to shoulder-surfing attacks. These exclude hybrid PIN-entry methods that require another factor (e.g., biometric behaviour) for authentication and the methods that employ other secrets (e.g., colours) besides digits. This inclusion criterion helps to answer the research questions.

IC2 Articles published in the English language; the reason for this choice is the difficulty of finding articles in other languages.

IC3 Primary research articles because systematic reviews are usually focused on them. This approach avoids reviews and editorial publications.

IC4 Full version and accessible articles to answer the research questions.

(c) ***Information sources***

Seven databases were identified as the information sources of the conducted SLR. These databases are ACM Digital Library, IEEE Xplore, Science Direct, Scopus, Web of Science, Wiley, and SpringerLink.

(d) ***Search Strategy***

Three key terms, “PIN", “shoulder surfing" and “recording attacks", were identified to find papers related to this SLR. A search string has been built based on these key terms and their variations as follows:

(“personal identification number" OR PIN) AND (“shoulder-surfing" OR "shoulder surfing" OR “shoulder-surf" OR “shoulder surf" OR “recording attack" OR “observation attack")

(e) ***Quality Assessment***

A quality assessment checklist of 11 criteria was designed to ensure that the findings of the selected articles can contribute to this SLR, as presented in Table 3.1. These criteria were developed based on the CASP Qualitative Checklist (2019) and the accumulated list presented by (Keele et al., 2007), which covers the design, data conduction, data analysis, and conclusion of a research article. To best of our knowledge, no consensus exists on the standard criteria to assess study quality. Thus, the aforementioned guides were utilised as some SLRs adopted them, and they cover all parts needed to evaluate the quality of a research article. A quality score is assigned for each assessed criterion: 1 for “fully meet", 0.5 for “partially meet", and 0 for “does not meet". The quality score of each article ranges from 0 to 11. Thus, an article with high score signifies high quality.

Table 3.1: Quality Assessment Criteria (Keele et al., 2007; Programme, 2019)

Design	1. Is the objective clearly stated?
	2. Is the PIN-entry method clearly described?
	3. Were research methods suitable to address the research aim?
	4. Were the study settings and sample justified and reproducible?
	5. Are the evaluation metrics used in the study fully defined?
	6. Are the evaluation metrics used in the study the most relevant?
Conduct	7. Was the data collection method(s) adequately described?
Analysis	8. Was the data analysis adequately described?
	9. Were the results compared with previous research?
Conclusion	10. Are the findings clearly stated and supported by the results?
	11. Are the research limitations presented?

(f) ***Data extraction strategy***

An Excel data extraction form was designed to extract the required data from the selected articles to address the research questions and quality assessment criteria. Table 3.2 shows the data items of this form and their description. The data extraction process was performed by one author.

3.2.1.2 Conducting Stage

The conducting stage represents the actual review of the literature. In this stage, the identification of the search is performed by searching the identified databases using the defined search string. This stage also includes the selection of the relevant studies, the quality assessment of these studies, and the extraction of the required data.

(a) ***Information Sources Search***

The search string was applied to seven databases: ACM Digital Library, IEEE Xplore, Science Direct, Scopus, Web of Science, Wiley, and SpringerLink. The reference list of the selected and review articles were also scanned for comprehension. CiteSeer^X and

Table 3.2: Data extraction from

Data Item	Description
ID	study identifier
Bibliographic info	title, year, author, source
publication type	journal, conference
study aim and objectives	aim and objectives of the study
PIN-entry method	direct input and indirect input
research methods	user study, security analysis, and others
study settings	design, sample size
evaluation metrics	measures used by the study
data collection	method of data collection
data analysis	method of data analysis
findings	results of the study
limitations	limitations of the study
comments	further comments on the study

Tylor & Francis online databases were excluded because they returned irrelevant results. Table 3.3 details the applied search fields and filters for each database. Searching on Wiley database was limited only to abstracts because title and abstract search returned 0 results. SpringerLink returned a huge number of irrelevant articles because it applies the search to the full text in addition to the title and abstract. Therefore, the results were sorted by relevance, and the most relevant ones (based on the title) were included for title/abstract screening. Furthermore, A search alert has been set on each database to get a notification by email when the saved search string (query) retrieves new results.

(b) ***Study Selection***

The study selection process was conducted as follows. Initially, the results of applying the search string to the identified databases were imported to EndNote software to manage the returned articles. Following this approach, the returned articles were checked for duplication and the duplicated ones were removed. Then, the results were filtered based on title, abstract, and keywords. The irrelevant articles were discarded. Finally, a partial or

Table 3.3: Search fields and filters for each database

Database	Search Fields	Refine by
ACM Digital Library	Title, Abstract, Keywords	-
IEEE Xplore	Title, Abstract, Keywords	-
ScienceDirect	Title, Abstract, Keywords	-
Scopus	Title, Abstract, Keywords	Conference paper, Article, English
Web of Science	Title, Abstract, Keywords	English
Wiley Online Library	Abstract	-
Springer Link	Titles, Abstract, Full Text	English

full reading of the articles was performed to remove the irrelevant ones and to extract the data needed to address the research questions and quality assessment criteria. All these steps were conducted by one author in accordance with the eligibility criteria. The same author performed a test-retest process where a random sample of the included and excluded articles has been re-evaluated to check the consistency of the study selection process.

(c) ***Data extraction***

The required data to answer the research questions and quality assessment criteria was extracted from the selected articles and stored in the excel data extraction form. The data extraction process was performed by one author. A test-retest approach was performed on a random sample of the selected articles to re-evaluate the reliability and consistency of the collected data, as Keele et al. (2007) recommended this approach for PhD students.

3.2.1.3 Reporting Stage

The last stage of the SLR was reporting the obtained results. These obtained results of the SLR were published in the Computer & Security journal.

(a) ***Study Selection Results***

A total of 765 articles were obtained from 7 databases; ACM Digital Library, IEEE Xplore, Science Direct, Scopus, Web of Science, Wiley, and SpringerLink. After removing

duplicate entries, we were left with 530 articles. Out of this number, 405 articles were discarded by screening the titles, abstracts, and keywords. Thus, 125 articles were included in the full reading. At the full reading scan, 71 out of the 125 articles were excluded: where 56, 10, and 5 articles do not match *IC1*, *IC3*, and *IC4* respectively. Only one article was included by scanning the reference lists of the selected and review articles. Therefore, the final set of selected articles in this review is 55. Figure 3.2 shows the review flow diagram of the study selection process.

(b) ***Study Characteristics***

The conducted SLR describes the most common features of the selected articles. Thirty-one of the selected articles were published in conferences, whereas the other 24 were published in scientific journals. The selected articles either used direct or indirect input method to resist shoulder-surfing attacks. Twenty-two of them used direct input methods, and 33 used indirect input.

The conducted systematic presents the evaluation results of the selected articles concerning the resistance to shoulder-surfing attack and recording attacks, PIN-entry time, and error rate. Some articles proposed more than one variation or setting of the PIN-entry method. The best performing method with respect to shoulder-surfing and recording attacks resistance and usability was selected. The selected articles proposed PIN-entry methods with varied resistance to shoulder-surfing and recordign attacks. Thus, they have been classified into “vulnerable" (not resistant to any captured session), “low" (resists only one captured session), “moderate" (partially resistant to multiple captured sessions), and “high" (fully resistant to multiple captured sessions). Most PIN-entry methods (37 out of 55) are highly resistant to shoulder-surfing attacks. Only four of them are still vulnerable to the attack, 13 PIN-entry methods with moderate resistance, and only one method provides low resistance. For recording-based shoulder-surfing attack, around one-third of

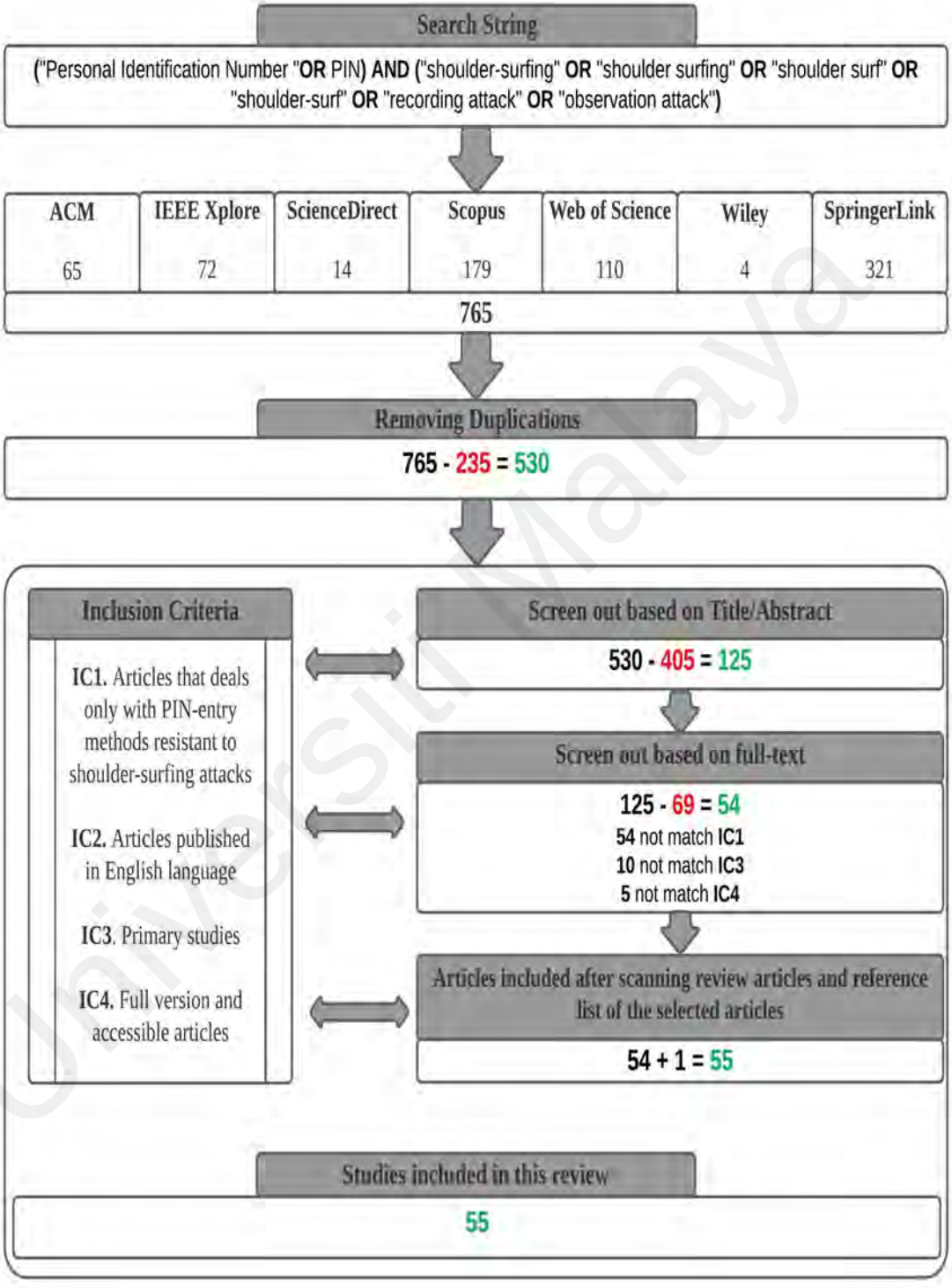


Figure 3.2: Study Selection Process

the PIN-entry methods are vulnerable (19 out of 55). Methods that are presented with high, moderate, and low resistance are 12, 16, and 8, respectively. All highly resistant methods assumed a secure channel to transfer the challenge. All PIN-entry methods resistant to recording-based shoulder-surfing attacks have the same level of resistance or higher to those resistant to human-based. In the same way, methods that are vulnerable to shoulder-surfing attacks are also vulnerable to the recording-based ones. Furthermore, all PIN-entry methods that are highly resistant to recording attacks employed indirect input methods to resist the attacks. A detailed discussion of these PIN-entry methods is provided in Chapter 2.

Usability evaluation is important when designing a secure PIN-entry authentication method because people are unwilling to accept a secure mechanism that affects the usability (Souza et al., 2018). In the selected studies, PIN-entry time and error rate are the most frequently adopted measures for usability. PIN-entry time is the time required to enter a PIN, and the error rate is defined as the rate of unsuccessful logins by a user. The number of articles that reported the PIN-entry time and error rate are 44 and 33, respectively. The lowest PIN-entry time was roughly 3 seconds. All except one of the studies that achieved the lowest PIN-entry time employed a direct input method. Most of the articles that employed the indirect input method required high PIN-entry time. For the error rate, 28 out of the 33 articles reported a success rate above 90%. Seven of them obtained a 100% success rate. A related point to consider is that a secure human executable protocol should enable people to perform computation with at least 90% success rate, in at most 10 seconds (Hopper and Blum, 2001, as cited in Chakraborty et al., 2019). Accordingly, only 11 methods matched the condition of the human executable protocol.

The conducted SLR presents the distribution of the selected articles based on the year of publication. Interestingly, research on PIN-entry methods resistant to shoulder-surfing

and recording attacks have received close attention since 2015. The SLR manifests that there is no study on this topic before 2004.

The research methods used by the selected studies are presented in Table 3.4. They are user study, security analysis, and usability analysis. The user study research method is the common one as it was used by most of the research articles (46 out of 55). It is employed to evaluate a method by testing it on users. Although some articles employed the user study method only to evaluate usability, it was used to evaluate security as well. Seventeen articles included a questionnaire with the user study, whereas only five articles included an interview. Both questionnaire and interview were used mainly to reflect user feedback in terms of usability and security of a PIN-entry method. There is only one study used a questionnaire to evaluate the usability of the PIN-entry method. Most of the user studies employed a range of 10–50 participants (30 were frequently used). Four articles with two each used a sample size below 10 and above 50 participants. Usability or security analysis refers to the method of analyzing usability or security measures of a system or method either qualitatively or quantitatively. Approximately half of the selected articles (29 out of 55) employed security analysis, whereas only 10 applied usability analysis.

Table 3.4: Research methods used by selected studies

Research Method	Evaluation Type	No. of Articles	Sample Size Details
User Study	Usability, Security	46 Total; 17 with Questionnaire, 5 with Interview	Most: 10–50 participants, 2 articles: < 10, 2 articles: > 50, Frequent: 30
Security Analysis	Security	29	N/A
Usability Analysis	Usability	10	N/A

(c) ***Quality Assessment Results***

Most of the articles (42 out of 55) scored a total of 7 or higher (out of 11), which is fair enough to make a valuable contribution to this review. Only three articles have a

low-quality score of 2 or less because they did not present the research method. All articles except S09 clearly stated the aim; however, none of them provided a justification of the sample size (i.e., none fully matched Q4).

(d) ***Research Questions Discussions***

The conducted SLR aimed to provide answers to the following research question and sub-questions:

What are the existent PIN-entry methods resistant to shoulder-surfing attack in the literature?

- What evaluation metrics were used to evaluate the PIN-entry methods?
- What are the limitations and open solutions/recommendations of the current PIN-entry methods?

Generally, the existing PIN-entry methods resistant to shoulder-surfing and recording attacks are classified into direct and indirect inputs. Direct input methods are categorised into visual distraction and gaze-based methods. The visual distraction methods include cursor camouflage, input distraction, and keypad distraction methods. Indirect input methods are classified into challenge-response and others. Challenge-response methods can also be classified into audio-based, haptic-based, and visual-based according to the channel used to send/receive the challenge. Chapter 2 presents more details about the existing PIN-entry methods resistant to shoulder-surfing and recording attacks.

Two main types of evaluation were adopted by most if not all selected articles - security and usability. The selected articles measured the security of PIN-entry methods in terms of resistance to shoulder-surfing and recording attacks, PIN-space, and self-reported security. Some articles reported the probability of attacks, such as timing and challenge-only attacks, in which an attacker analyses the recorded user's response time and challenge to obtain the

actual PIN. These attacks could be part of the recording attacks as attackers analyse the recorded authentication sessions to identify the PIN. The resistance to shoulder-surfing and recording attacks were evaluated by 31 and 23 selected studies, respectively. PIN-space is the number of unique PIN combinations that can be created from digits. It was used by 20 articles to calculate the success probability of guessing attacks. The self-reported security evaluation metric was obtained by the questionnaires, interviews, or both that conducted on participants as part of the user studies (reported by eight studies).

Regarding usability evaluation, the selected articles used a total of nine evaluation metrics. Error rate and PIN-entry time were the most frequently used by 33 and 42 of the selected articles, respectively. The error rate is classified into basic and critical. The basic error rate is measured as the number of failed login attempts, whereas the critical error rate is measured as the entirely failed authentication sessions. Generally, a maximum of three attempts was allowed for each participant per authentication session to be logged as a failed session. Thirty-one of the selected articles employed the basic error rate, eight articles employed both, and two employed only the critical one. The PIN-entry time is the time required by a user to enter his or her PIN. The PIN-entry time and error rate are essential measures for the adoption of a PIN-entry method. Only 11 methods matched the condition of the human executable protocol (people perform authentication within 10 seconds, with at most 10% error rate), as mentioned in previous section. Four of them are categorised under direct input methods, whereas the others are categorised under indirect input methods.

Other usability evaluation metrics are learning effect, mental workload, and user feedback. Six articles reported the learning effect evaluation metric. All except one study measured the learning effect among participants through the PIN-entry time, after a number or days of interactions with the proposed PIN-entry methods. The excepted

study presented a qualitative analysis to report the learning effect. Six articles analysed the mental workload, which is about the mental effort (including memory burden) required by a user to key in his or her PIN. User feedback includes five measures: ease of use, familiarity, likelihood of future usage, self-reported usability, and user satisfaction. They were measured by asking participants through questionnaires and/or interviews. Other articles include cost and PIN compatibility evaluation metrics. Only one article reported the cost, and two articles reported the PIN compatibility. a PIN-entry method is cost-effective when it requires no additional equipment. To ensure the acceptance and adoption of a PIN-entry method, it has to be compatible with the conventional PIN-entry method in the sense that it requires no additional channel and uses a 4-digit PIN.

Overall, the SLR argues that none of the compatible PIN-entry methods provides high resistance for both shoulder-surfing and recording attacks. It emphasises that future studies should focus on the development of compatible and usable PIN-entry methods resistant to shoulder-surfing and recording attacks to ensure their acceptance and adoption. The outcome of this phase led to the establishment of the research problem and directed the focus towards the design of a PIN-entry method resistant to shoulder-surfing and recording attacks.

3.2.2 Phase2: Proposed PIN-Entry Method Design

The second phase aims to design a PIN-entry method resistant to shoulder-surfing and recording attacks in order to accomplish the second research objective. To do so, an indirect input PIN-entry method using challenge-response is proposed. The challenge-response approach relies on the addition mod 10 with a mini-challenge keypad in order to produce a OTP password that obscures the original PIN. The rational behind using the addition mod 10 is have an equal probability of response digits in order to resist shoulder-surfing and recording attacks (Kwon & Hong, 2015). Therefore, it is employed to produce equally

likely OTP digits so as to remove any correlation between authentication sessions, and hence, attackers will fail to recover any PIN due to the difficulty of identifying the original PIN digits.

To perform the authentication, a user needs to do a simple mod 10 addition of the PIN and challenge digits in order to produce the OTP. The reason behind the employment of the addition mod 10 is to produce equally likely OTP digits. For instance, let the OTP entered by a user be 1135. So the digit 1 in the OTP could be resulted from the 1 + 0 mod 10, 2 + 9 mod 10, 3 + 8 mod 10, 4 + 7 mod 10, 5 + 6 mod 10, and vice versa. The digit 3 in the OTP could be resulted from the 3 + 0 mod 10, 4 + 9 mod 10, 5 + 8 mod 10, 6 + 7 mod 10, 2 + 1 mod 10, and vice versa. The digit 5 in the OTP could be resulted from the 5 + 0 mod 10, 6 + 9 mod 10, 7 + 8 mod 10, 1 + 4 mod 10, 2 + 3 mod 10, and vice versa. It can be noted that all digits from (0, 1, 2, ..., 8, 9) are equally likely to be true for each digit of either the PIN or the challenge. Therefore, the generated OTP obscures the original PIN as well as the challenge digits.

Three versions or designs of the proposed PIN-entry method are presented so as to find the best one. The first version of the proposed PIN-entry method displays the addition mod 10 table as a matrix (rows and columns). In contrast, the second version of the proposed PIN-entry uses the regular keypad layout to display the addition mod 10 table. The underlying rational for the second design or version is that people might not familiar with the first design (i.e., matrix keypad). Thus, the regular keypad layout is employed to display the addition mod 10 table. Apart from displaying the addition mod 10 table as a keypad, the third proposed PIN-entry method maintains the same layout as the regular PIN keypad. It only requires a simple human computation of the addition mod 10 instead of displaying its table. Diagrams and pseudo code were used to describe these versions of the proposed PIN-entry method.

3.2.3 Phase3: Prototype Implementation

Based on the design of the proposed PIN-entry method in the previous phase, this phase involves the achievement of the third research objective of implementing prototypes of each version of the proposed PIN-entry method. In addition, a prototype of the regular PIN-entry method was developed. A use case diagram was used to model the registration, login, and storage of each version of the proposed PIN-entry method. The use case diagram provides a graphical depiction of how a user interacts with the registration, login, and storage models of the proposed PIN-entry authentication method. These models were developed using Python and SQLite. The registration and login models were developed using the Python language, and SQLite was used as a database for the developed models. Visual Studio Code was used as the development tool.

3.2.4 Phase4: Evaluation and Analysis

The purpose of the fourth phase is to evaluate and analyse the proposed PIN-entry method in order to achieve the fourth research objective. Two user studies, preliminary and primary, were conducted to evaluate the effectiveness of the proposed PIN-entry method in terms of shoulder surfing and recording attacks. The conducted SLR manifests that the user study is the most viable research method that was used by research articles to evaluate the security and usability of a PIN-entry method. In the user study, a prototype of the proposed PIN-entry method is evaluated by testing it on users. The SLR also shows that some articles included questionnaires and interviews with the user studies. Thus, a questionnaire and interview were included with the user studies in order to evaluate the proposed PIN-entry method in this research work.

Initially, a preliminary user study was conducted to analyse all three versions of the proposed PIN-entry method in terms of security, usability, and user perception in order to find the best one. The third version was preferred by all participants and had the best

usability. Thus, the third version was evaluated in the primary user study with the regular PIN-entry method and related work. Thirty participants (9 females) were recruited to conduct both studies. All the participants were students, and they were aged between 11 and 38. Participants were given three attempts per authentication session.

The user studies were conducted in three phases: training, testing, and feedback. The training phase was started by explaining the purpose of the study and the procedures and task scenarios for each PIN-entry method. Following that, the participants were given free training to get ready for the test. They were also asked to fill out a demographic information form before the test. Table 3.5 shows the details of the participants' demographic information. In the testing phase, participants were asked to enter their PINs while attackers were observing the authentication sessions. The user studies were concluded with the feedback phase. In the preliminary user study, participants were interviewed about the best version and why, whereas they were asked to fill out a questionnaire in the primary user study.

Table 3.5: Participants Demographic Information Form

No.	Input field
1	Name
2	Gender
3	Age
4	What is your level of education?
5	Are you familiar with PIN-entry method?

There were three main statistical analysis methods used in the evaluation: percentage, mean, and t-test. The percentage was used to report the successful attacks and error rate. The percentage of successful attacks was used to measure the effectiveness of the proposed PIN-entry method in mitigating shoulder-surfing and recording attacks. The error rate percentage was used to report the number of failed login attempts. To determine the overall

PIN-entry time, the mean was used. The t-test analysis was used to determine if there was a significant effect of the PIN type and PIN method.

3.3 Chapter Summary

This chapter describes the research methodology adopted to achieve the research objectives of this work. It presented a framework with four successive phases: systematic review, proposed PIN-entry method design, prototype implementation, and evaluation and analysis. Each phase discusses the methods and outcomes associated to a one research objective. The next chapter presents the proposed PIN-entry method.

CHAPTER 4: PROPOSED PIN-ENTRY METHOD

4.1 Introduction

This chapter presents the proposed PIN-entry method resistant to shoulder-surfing and recording attacks. It begins by giving a brief overview of the proposed PIN-entry method. Then, three versions of the proposed PIN–entry method are discussed. There are two main processes for each version: registration and login. The registration process is similar to the regular PIN-entry method for all versions. The login process is different for each version. The implementation details of the proposed PIN-entry method, including the two processes, are illustrated with the help of a use case diagram.

4.2 Overview of the Proposed PIN-entry Method

To achieve the second objective of this research, a PIN-entry method resistant to shoulder-surfing and recording attacks has been proposed. The proposed PIN-entry method employs an indirect input method of entering the PIN using the challenge-response approach. In challenge-response PIN-entry methods, a user is given a challenge. Then, he or she needs to find and input the response based on his or her knowledge of the challenge and the original PIN. As a result, the user enters a one-time response per session to reduce the threat of shoulder-surfing and recording attacks. The challenge could be sent to the user through an audio, haptic, or visual channel of communication.

The proposed PIN-entry method relies on the addition mod 10 with a challenge keypad in order to produce a one-time PIN (OTP) that obscures the original PIN. When employing a challenge-response PIN-entry method, the challenge must be unknown and the likelihood of response digits must be equivalent in order to resist shoulder-surfing and recording attacks (Kwon & Hong, 2015). The addition mod 10 can be used to have an equal probability of response digits (J.-H. Kim et al., 2017; Seo et al., 2017). Therefore, it is employed to

produce equally likely OTP digits so as to remove any correlation between authentication sessions and thus resist shoulder-surfing and recording attacks. The challenge keypad is a mini random digit keypad that is used to locate the challenge digits. It is delivered through the same visual channel that is used to deliver the response. The challenge digits are identified through the knowledge of the PIN digits.

It is remarkable that the proposed PIN-entry method is unimodel method in which the same visual channel of communication is used to transfer the challenge and deliver the response. Thus, this could give such method more preferences than bimodal challenge–response methods (i.e., audio-based and haptic-based) in terms of simplifying the login process and maintaining the regular PIN-entry method compatibility. Besides, a user needs only to remember the PIN digits to identify the challenge digits. This is also compatible with the regular PIN-entry method, where no information is required to be memorised except the PIN.

4.3 Versions of the Proposed PIN-entry Method

Three versions of the proposed PIN-entry method are presented according to the way of using the addition mod 10 to produce the OTP. The reason behind proposing different versions is to find the best design that ensures the acceptance and adoption of the proposed PIN-entry method. There are two main processes in each version of the proposed PIN-entry method: registration and login. The registration process is similar to the regular PIN-entry method for all versions, while the login process is different.

4.3.1 Registration Process:

The user registers a username and creates a PIN password (4 or 6 digits) during the registration process. The registration process is assumed to be secure. It is the same for all versions of the proposed PIN-entry method.

4.3.2 Login Process:

The user has to provide his or her username (i.e., ID) and OTP during the login process. Figure 4.1 shows the user's login into the system. First, the user types in his or her username. Then, the server sends R in the form of the challenge keypad. Finally, the user must calculate or find out the OTP and send it to the server. The details of how the user derives and enters the OTP for each version are described in the next sections.

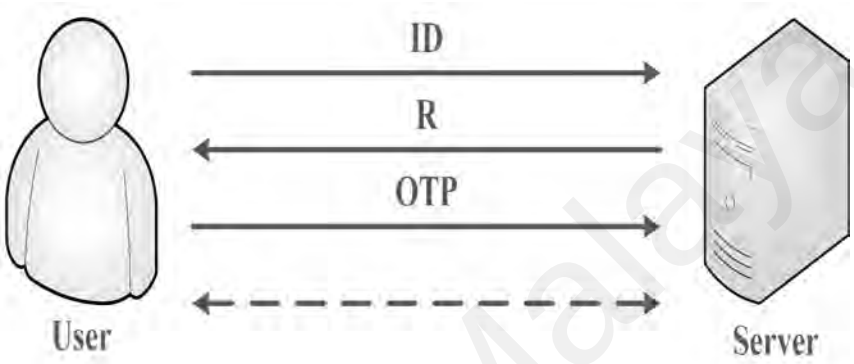


Figure 4.1: Login Phase

4.3.2.1 First version

The first version of the proposed PIN-entry method displays the addition mod 10 table as a matrix (rows and columns), as shown in Figure 4.2. The top row represents the challenge keypad used to identify the challenge digits. The challenge digits are the same as the PIN digits but with the present order on the top row. The sequencing requirement of the challenge digits is marginalised to avoid session correlation and make it difficult for an attacker to predict the original PIN. To produce the OTP, the user needs to intersect the PIN digits located on the leftmost column with the challenge digits located on the top row. For instance, let Figure 4.2 represents the keypad sent by the server for authentication. Suppose the user's PIN is 1472, then the challenge digits are 7142 according to their present order on the top row. The intersection of the first digits of the PIN (i.e., 1) and the challenge (i.e., 7) is 1. The intersection of the second digits of the PIN (i.e., 4) and the

challenge (i.e., 1) is 6. The intersection of the third and fourth digits of the PIN (i.e., 7 and 2) and the challenge (i.e., 4 and 2) are 4 and 1, respectively. Therefore, the user needs to enter the OTP of 1641 to login.

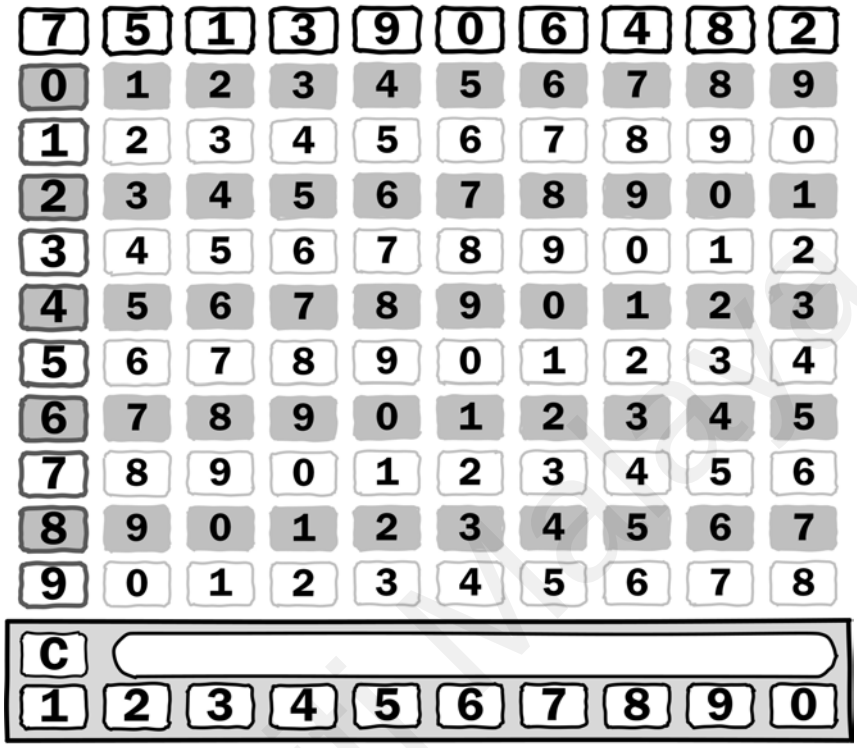


Figure 4.2: The keypad of the first version of the proposed PIN-entry method

Algorithm 1 describes the login procedure on the server-side. The server first calculates the otp_server based on the index of the challenge (R) on the top row (index starts at zero) and the stored PIN (P), as shown in equation 4.1. The server grants access to the user only if otp_server matches the user's OTP that is taken as input.

$$OTP = (P + index(R)) \mod 10 \tag{4.1}$$

4.3.2.2 Second version

The first version of the proposed PIN-entry method displays the addition mod 10 table as a keypad to locate and enter the OTP. However, users might not be familiar with such a keypad. So, the second version of the proposed PIN-entry method uses the regular keypad

Algorithm 1: Login procedure on server (first and second versions)

Input : OTP as an array of 4 elements
Output : Grant access or wrong password

Initialize: otp_server = [], X = 0;
for $i = 0$ **to** 3 **do**
    $otp\_server[i] = (P[i] + index(R[i]))$ mod 10;
end
for $j = 0$ **to** 3 **do**
    if $otp\_server[j] = OTP[j]$ **then**
        $X \leftarrow 1$;
    else
        $X \leftarrow 0$;
        break;
    end
end
if $X == 1$ **then**
    grant access;
else
    wrong password;
end

layout to display the addition mod 10 table, as shown in Figure 4.3. It resembles the regular keypad in order to improve usability. To perform authentication, the user needs to locate the challenge digits on the challenge keypad located at the bottom right. The challenge digits are the same as the PIN digits but with the present order on the challenge keypad. Then, the user corresponds the challenge digits on the PIN digits' mini keypads to derive the OTP. Suppose the user created a PIN of 1427; the challenge then is 7142 according to Figure 4.3. To produce the OTP, the user corresponds the first digit of the challenge (i.e., 7) on the mini keypad of the first PIN digit (i.e., 1). So, the first digit of the OTP is 1. Then, the user repeats the same process with the second digit of the challenge (i.e., 1) on the mini keypad of the second PIN digit (i.e., 4) to produce the second digit of the OTP (i.e., 6). The third and fourth digits of the OTP are 4 and 1, respectively. On the server-side, the second version is similar to the first version, where Algorithm 1 is used to model the login process.

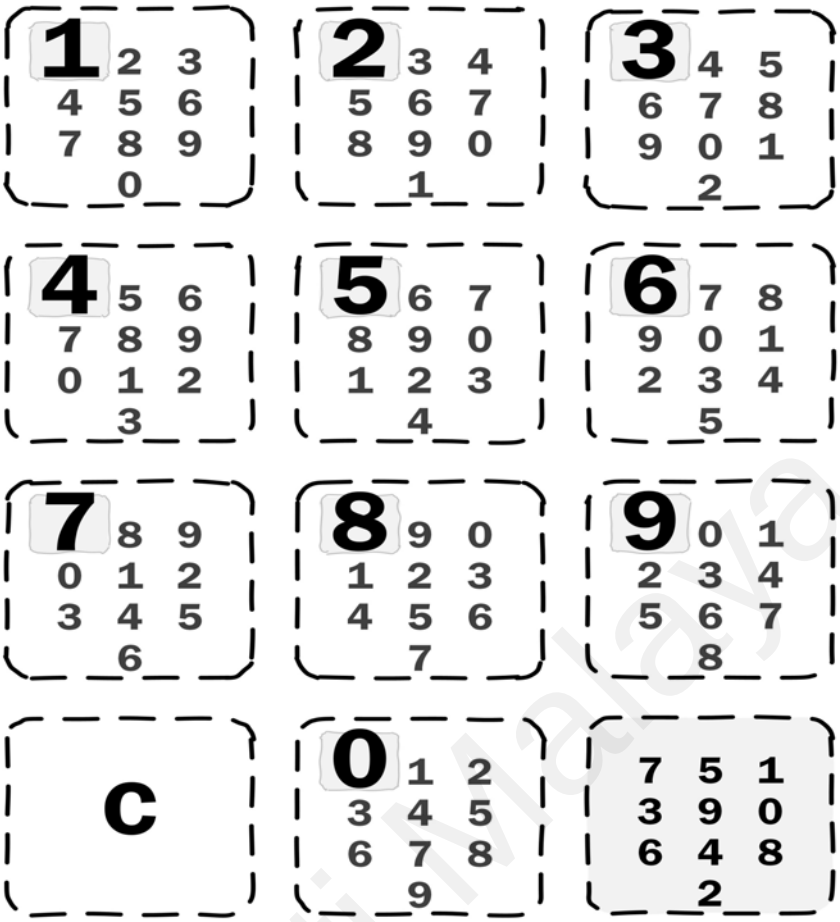


Figure 4.3: The keypad of the second version of the proposed PIN-entry method

4.3.2.3 Third version

The first and second versions of the proposed PIN-entry method display the addition mod 10 table as a keypad in order to help users derive and enter the OTP. However, users might be unfamiliar with such keypads, and they (i.e., keypads) might confuse the users due to the large decoy digits. Therefore, the third version of the proposed PIN-entry method requires simple human computation of the addition mod 10 instead of displaying its table. Figure 4.4 shows the keypad layout of the third version. It uses the same regular keypad to maintain compatibility. The only difference is the presence of a mini-challenge keypad at the bottom-right that is used to locate the challenge digits.

The challenge, R, is a random number composed of the same length of digits as the original PIN. To derive it, a user needs to map the PIN key location on the challenge

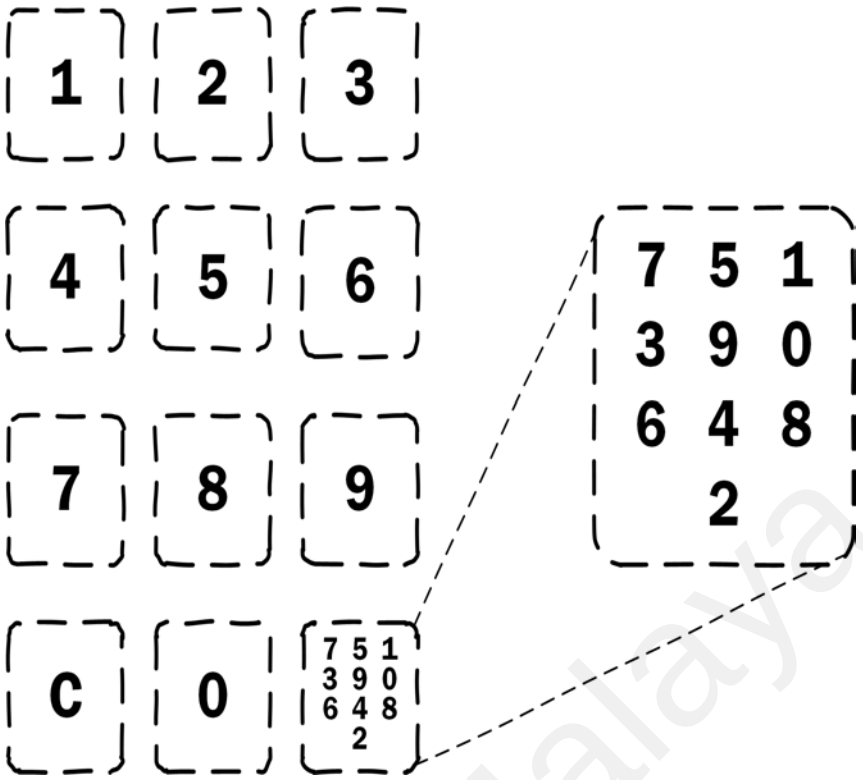


Figure 4.4: The keypad of the third version of the proposed PIN-entry method

keypad. R digits should be ordered according to the key locations of the PIN digits on the regular keypad layout (i.e., 1, 2, 3, ..., 9, 0) to avoid sessions correlation and thus make it difficult for an attacker to predict the original PIN. For example, suppose the user creates a PIN of 1472. As in Figure 4.4, the R digits are 7, 3, 6, and 5. The digit 5 of the R digits results from mapping the digit 2 (fourth digit) of the PIN with its key location on the challenge keypad. In this version of the proposed method, the sequence of the R digits needs to be rearranged in ascending order based on the key locations of the PIN digits on the regular keypad layout (i.e., 1, 2, 3, ..., 9, 0) to prevent the correlation between the authentication sessions of "correlation of the numbers". Therefore, the digit 5 of the R needs to be placed before the digits 3 and 6 because digit 2 precedes digits 4 and 7 of the PIN on the regular keypad layout. Therefore, R is 7536.

To perform the authentication, the user needs to produce the OTP based on the addition mod 10 formula that takes two parameters, the original PIN P and the challenge R, as

shown in equation 4.2. Suppose P is 1472, then the OTP is 8908 according to Figure 4.4. Likewise, the server calculates otp_server and grants access to the user if otp_server matches the OTP entered by the user, as described in Algorithm 2.

Algorithm 2: Login procedure on server (third version)

```
Input  : OTP as an array of 4 elements
Output : Grant access or wrong password
Initialize: otp_server = [], X = 0;
for i = 0 to 3 do
    otp_server[i] = (P[i] + R[i]) mod 10;
end
for j = 0 to 3 do
    if otp_server[j] = OTP[j] then
        X ← 1;
    else
        X ← 0;
        break;
    end
end
if X == 1 then
    grant access;
else
    wrong password;
end
```

$$OTP = (P + R) \mod 10 \tag{4.2}$$

4.3.2.4 Error attempts

If the user enters a wrong PIN many times (i.e., violate the threshold), the system asks the user to attempt authentication after a certain time. If he or she failed again, the system would lock the account. The user then needs to contact the system administrator for the procedures required (e.g., requesting a security code through email or phone number) to unlock his or her account. The reason for locking the user's account is to avoid a guessing attack. In fact, repeatedly entering a wrong password is a sign of an attack. The recovery phase is similar to traditional password-based authentication, where the user resets the

password if it is forgotten.

4.4 Prototype Implementation of the Proposed PIN-Entry Method

To achieve the third objective of this research, prototypes of the regular PIN and each version of the proposed PIN-entry methods have been developed for testing and evaluation purposes. This section describes the prototype implementation of the proposed PIN-entry method. It is the same for regular PIN-entry and all versions of the proposed PIN-entry methods. A use case diagram is used to illustrate the implementation and function requirements of the registration and login processes. The Python programming language was used to model the registration and login processes. SQLite was used as a database for the developed methods.

4.4.1 Use Case Diagram of the Proposed PIN-Entry Method

As illustrated in Figure 4.5, the use case diagram is used to depict how a user interacts with the proposed PIN-entry method. There are two main processes of the proposed PIN-entry method: registration and login. Each has a separate Python file. There are also two Python files, one for the main window and the other for managing the database. The main window of the prototype displays the registration and login process buttons. The registration process includes setting a username and PIN. The system restricts the user's input in terms of value and length. It displays a registration error in the case of keeping either the username or PIN fields empty.

The login process includes entering and verifying the username, entering and verifying the PIN, and displaying the login error. The username is required to keep track of the users in terms of successful and failed attempts and PIN-entry time. Entering the PIN involves generating the challenge and showing the keypad. The challenge is generated randomly for each authentication session. The keypad is shown according to the version

of the proposed PIN-entry method. Verifying the PIN includes implementing the login procedure algorithm of the proposed PIN-entry method. An invalid username or PIN error message is displayed in the case of entering a nonexistent username or a wrong PIN, respectively.

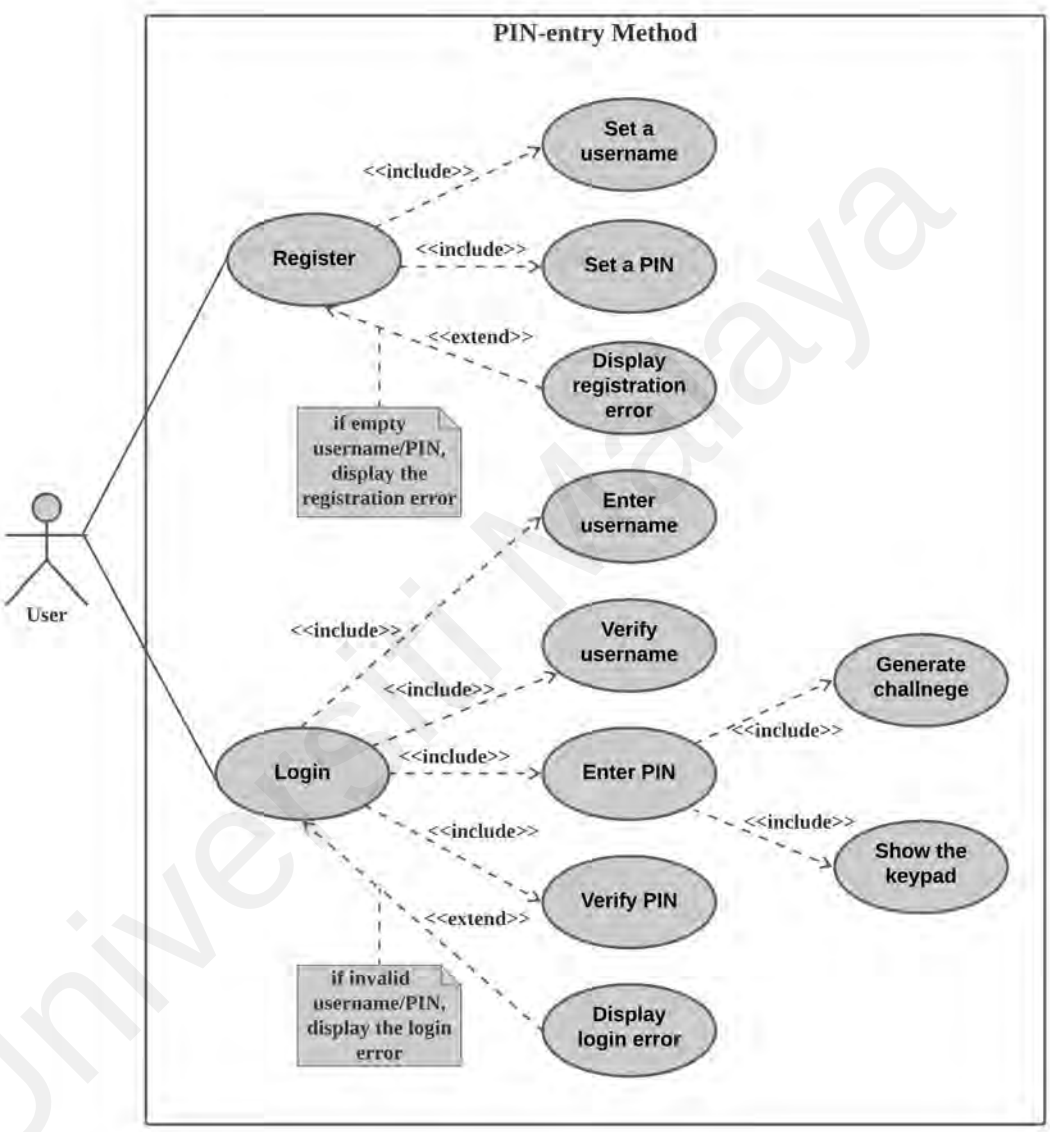


Figure 4.5: Use case diagram of the proposed PIN-entry method

4.4.2 Database Design

Table 4.1 shows the database metadata for the proposed PIN-entry method. It defines 14 fields:- username, PIN, failed_attempt, failed_auth, and time1, time2, ..., time10. The username is used to identify the user. The PIN field stores the user's PIN. The

failed_attempt field is used to count the failed attempts. The failed_auth field is used to count the failed authentication sessions. The user is given three attempts per authentication session. If the user fails all three attempts, the authentication session is marked as failed, and so the failed_auth is incremented by 1. The users of the user study were asked to enter their PINs 10 times, with three attempts per entry. Therefore, time1, time2, ..., and time10 are used for logging the user's PIN entry time for the first entry, second entry, ..., and tenth entry, respectively.

Table 4.1: Database metadata

Field Name	Type	Null	Key	Description
username	text	No	PRI	defines user's identity
PIN	integer	No	-	stores user's PIN
failed_attempt	integer	No	-	counts failed attempts
failed_auth	integer	No	-	counts failed authentication session
time1 ... time10	integer	No	-	logs PIN-entry time

4.5 Chapter Summary

This chapter presents the proposed PIN-entry method resistant to shoulder-surfing and recording attacks. In addition to highlighting the main remarkable points, it provides an overview of how the proposed PIN-entry method works and resists these attacks. Three versions of the proposed PIN-entry are proposed. There are two main processes for each version: the registration process and the login process. The registration process is the same for all versions, whereas the login process is different. The details of how a user logs in using each version are illustrated using figures and algorithms. The proposed PIN-entry method employs a challenge-response approach using the addition mod 10 and a challenge keypad to produce an OTP. The OTP hides the the original PIN in order to resist shoulder-surfing and recording attacks. The prototype implementation of the proposed PIN-entry method is described with the help of the use case diagram. This chapter includes

information about the database design of the proposed PIN-entry method. The evaluation and analysis of the proposed PIN-entry method are presented in the next chapter.

CHAPTER 5: PRELIMINARY USER STUDY

5.1 Introduction

This chapter presents the preliminary user study conducted to analyse the three versions of the proposed PIN-entry method according to security, usability, and user perception. The purpose of this preliminary user study is to find the best version of the proposed PIN-entry method before comparing it with the regular PIN and related work. The security analysis of these versions was performed through their resistance to shoulder-surfing and recording (video-based and spyware-based) attacks. The usability analysis was measured using PIN-entry time and error rate. This chapter also describes the interview undertaken to report the user perception towards the best version of the proposed PIN-entry method.

5.2 Experimental Settings

A preliminary user study, including an interview, was conducted to find the best version of the proposed PIN-entry method. A 3x2 within-subject design was conducted to evaluate the security and usability of each version of the proposed PIN-entry method. The within-subject design is used to reduce the error variance associated with individual differences between participants, where all participants try all conditions. That is, each participant enters easy and hard PINs using each version of the proposed PIN-entry method. There are two independent variables in the 3x2 design: the PIN method and the PIN type. The PIN method has three levels (version1, version2, version3), and the PIN type has two levels (easy and hard). The order of the conditions was counterbalanced to reduce the learning effect. Participants were given three attempts per authentication session. To keep the proposed PIN-entry method simple, a 4-digit PIN is proposed.

PINs are categorised into hard and easy according to the number of distinct or identical digits. The hard PIN has at least three distinct digits, while the easy PIN has at most

Table 5.1: PIN Types and Patterns

PIN Type	PIN Pattern and Variations		Example
	Pattern	Variation	
Hard	Four distinct digits	–	2345
	Three distinct digits	Nonconsecutive identical digits	2321
		Consecutive identical digits	2231
Easy	Two distinct digits	Nonconsecutive identical digits	2121
		Consecutive identical digits	2211
	Three identical digits	Nonconsecutive identical digits	2212
		Consecutive identical digits	2221
	Four identical digits PIN	–	2222

two. Table 5.1 presents the details of PIN types and patterns. The reason behind this categorisation is to measure the effect of each PIN type on the proposed PIN-entry method's security and usability. Easy PINs are assumed to be easy to enter and detect because they have at most two distinct digits and always produce two distinct OTP digits (except for the 4-identical digits pattern). On the contrary, hard PINs are assumed to be hard to enter and detect because they have at least three distinct digits and can produce equally likely OTP digits.

5.3 Participants

Thirty participants (nine females) were recruited to conduct this study. The possibility of recruiting more and diverse participants was difficult due to the restriction imposed during the Covid 19 pandemic. Nonetheless, thirty participants were the most common in user studies (Binbeshr et al., 2020). In addition, a sample size of 30 participants can provide significant results for a comparative user study. For instance, Alroobaea and Mayhew (2014) suggest that a group size of 12 to 25 participants typically provides valid results. Six and Macefield (2016) found that a sample size of 20 participants or more is valid for comparative studies or studies that seek statistically significant findings. All

participants were students from different levels and different disciplines, and they had experience with the regular PIN-entry method. They were aged between 18 and 38. It is deemed appropriate for studying this type of population as they often experience a variety of situations with regular PIN. Moreover, students are commonly employed to conduct user studies (Lazar et al., 2017)

5.4 Procedure

The user study was conducted in three phases: training, testing, and feedback. The training phase was started by explaining the purpose of the study and the procedures and task scenarios for each PIN-entry method. The next step was to provide free training for participants until they were ready for the test. Prior to the test, participants were asked to fill out a basic demographic information form in order to attain a sufficient context of the study.

In the testing phase, each participant was asked to enter two PINs (easy and hard) using each PIN-entry method three times. Each login is marked as successful if the participant passes the test within three trials. For later analysis, the PIN-entry time and error rate were logged. The user study was concluded with the feedback phase. In this phase, participants were interviewed about which proposed PIN-entry method they preferred and why.

A pilot study was conducted to find the most appropriate attackers for conducting the attacks. First, the participants were surveyed about their familiarity with PIN-entry methods, shoulder-surfing, and recording attacks. Then, those who reported their familiarity were tested. Only two of them were found capable of conducting and implementing all the attacks. The two attackers were free to move in order to find the best position to perform the shoulder-surfing attack. To implement the video-based recording attacks, all authentication sessions were recorded using a camera. For spyware-based recording attacks, the attackers have access to the recorded videos and the user input (i.e., OTP). The attackers had full

control of the recorded videos for the purpose of guessing the original PINs. All attacks were based on three views followed by three guesses per view.

5.5 Security Analysis

This section analyses the security of the three versions of the proposed PIN-entry method against shoulder-surfing and recording attacks (video-based recording, spyware-based recording). To evaluate the proposed PIN-entry method versions against shoulder-surfing attack, the attackers stand in the user's vicinity and observe the authentication session multiple times. They were allowed to use a pen and paper to take notes. Figure 5.1 shows that all versions of the proposed PIN-entry methods provide the same security level in resisting shoulder-surfing attacks. The shoulder surfers failed to recover any hard PIN, while they were able to recover 16.67% of the easy PINs.

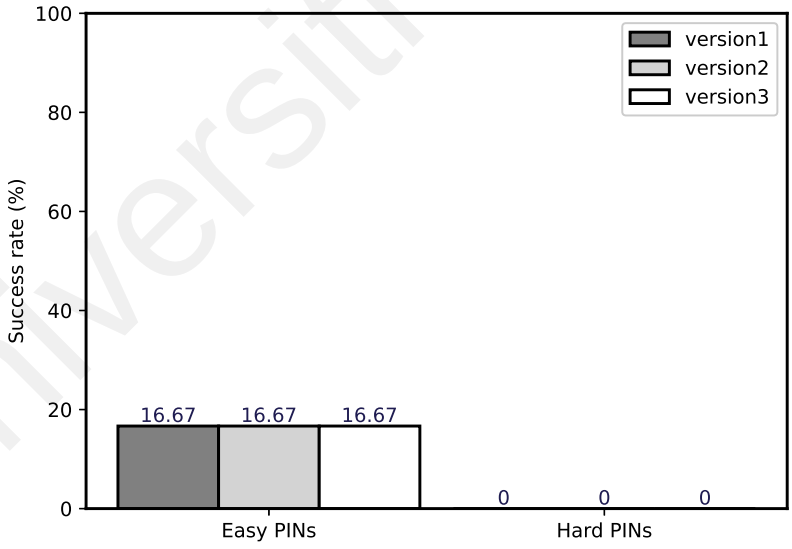


Figure 5.1: Shoulder-surfing attack success rate on easy and hard PINs of the three versions of the proposed PIN-entry method

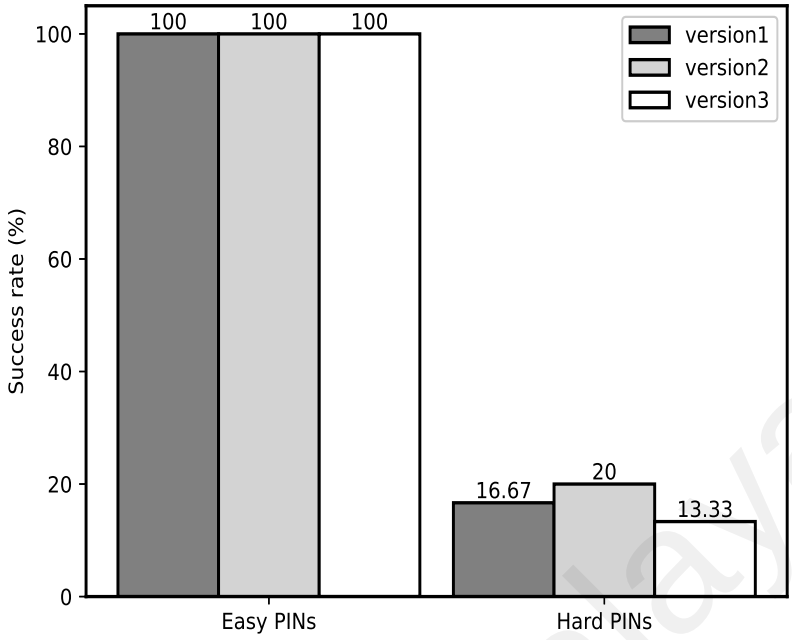
In the video-based recording attack, a camera device was employed to record the user's authentication sessions. The attackers had full access to watch these recorded videos in order to reproduce the original PIN. In the spyware-based recording, the attackers were

given the user input (i.e., OTP) in addition the recorded videos. Figure 5.2 shows that both video-based and spyware-based recording attacks failed in most hard PIN cases, while they were successful in all cases of easy PINs. It should be noted that all versions provide the same level of security in resisting such attacks. The slight variations in the success rate of hard PINs between the versions are caused by the random distribution of the challenge digits. The more detailed analysis is presented in Chapter 6.

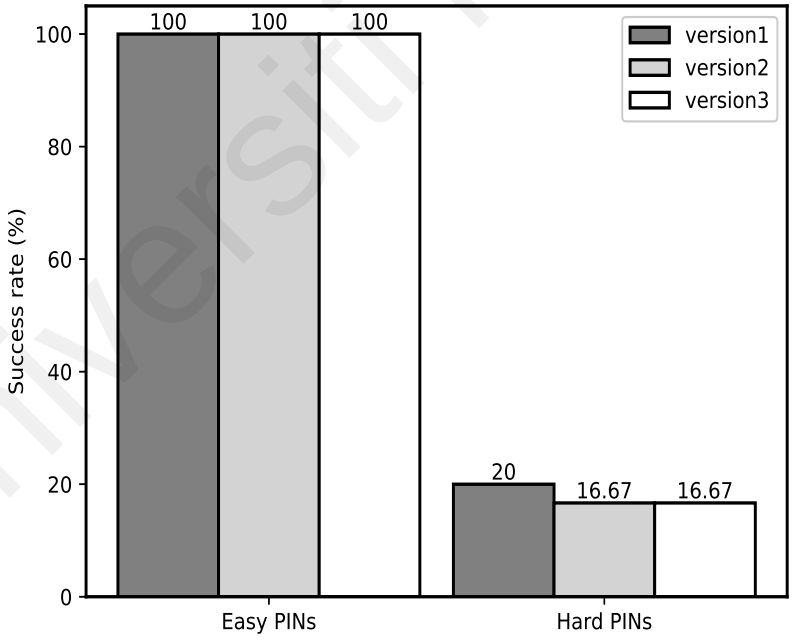
5.6 Usability Analysis

The usability of the proposed PIN-entry method versions was measured using PIN-entry time and error rate. These metrics are widely used in the literature to evaluate the usability of PIN-entry methods (Binbeshr et al., 2020). The PIN-entry time was measured as the time a user takes to enter his or her 4-digit PIN. The error rate was classified into basic and critical. The basic error rate was measured as the number of failed login attempts for successful authentication sessions; the critical error rate was measured as the number of entirely failed authentication sessions. A paired sample t-test was used to measure the effect of the PIN type as well as the PIN methods. A $p < 0.05$ is used for statistical significance level.

Figure 5.3 shows the average PIN-entry time for all three versions of the proposed PIN-entry method. It is noted that the average PIN-entry time of the third version is significantly faster than the first and second versions for the hard PIN type and both types (easy and hard), respectively ($p < 0.05$). The participants took a shorter time to enter their PINs using the third version of the proposed PIN-entry method due to the easiness of OTP derivation. In particular, participants refer to the keypad of the third version only to locate and identify the challenge digits and then compute the OTP on the fly. On the other hand, they refer to the keypad of the first and second versions to locate and identify the challenge digits and derive each digit of the OTP too. This results in a slowing of their PIN-entry



(a) Success rate of video-based recording attack



(b) Success rate of spyware-based recording attack

Figure 5.2: Recording attacks success rate on easy and hard PINs of the three versions of the proposed PIN-entry method

time. Similarly, the third version (hard PIN) is less erroneous than the other versions due to the OTP derivation and entering, as shown in Figure 5.4.Alesand, E For the critical

error rate, none of the participants failed any authentication session (i.e., all three attempts) for all three versions.

5.7 User feedback

The user feedback was collected using an interview in order to report the participants' perception toward the best version of the proposed PIN-entry method. The participants were interviewed about which proposed PIN-entry method they preferred and why. All participants reported that the third version of the proposed PIN-entry method is preferred because of its ease of OTP derivation and entering. This result goes along with the reported results of the usability tests in terms of PIN-entry time and basic error rate.

5.8 Chapter Summary

This chapter examines the preliminary user study that was conducted in order to determine the best version of the proposed PIN-entry method before comparing it to the regular PIN and related work. The proposed PIN-entry method versions were evaluated based on their security, usability, and user perception. The resistance of the three versions of the proposed PIN-entry method to shoulder-surfing and recording (video-based and spyware-based) attacks was used to assess their security. The security analysis results show that all three versions provide the same level of security. The analysis of the PIN-entry time and error rate reveals that the third version of the proposed PIN-entry method outperforms the first and second versions in terms of usability due to the ease of OTP derivation. This chapter also goes over the interview that was conducted to report on the participants' perceptions of the best version of the proposed PIN-entry method. The third version was preferred by all participants due to its ease of OTP generation and entry. In a nutshell, the preliminary user study found that the third version was more usable than the others and was preferred by the participants. As a result, the third version was chosen for the primary

user study, where it was compared to the regular PIN-entry method and related work.

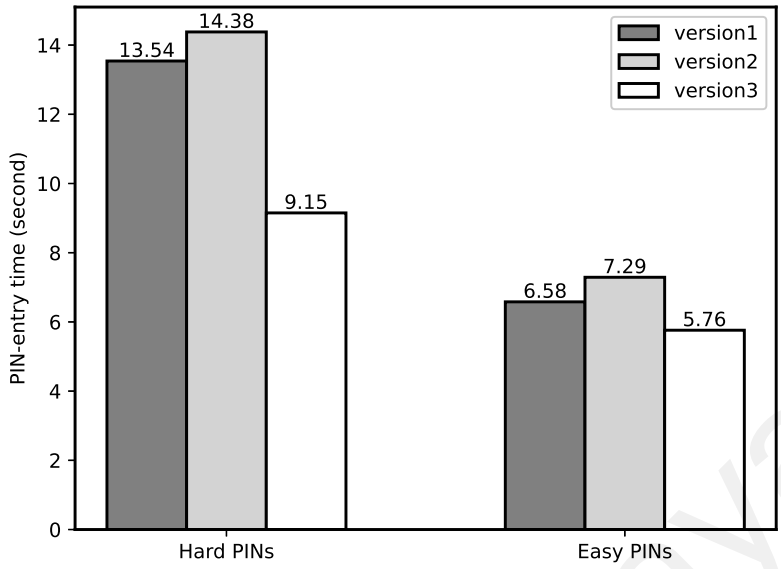


Figure 5.3: PIN-entry time for easy and hard PINs of the proposed PIN entry method versions

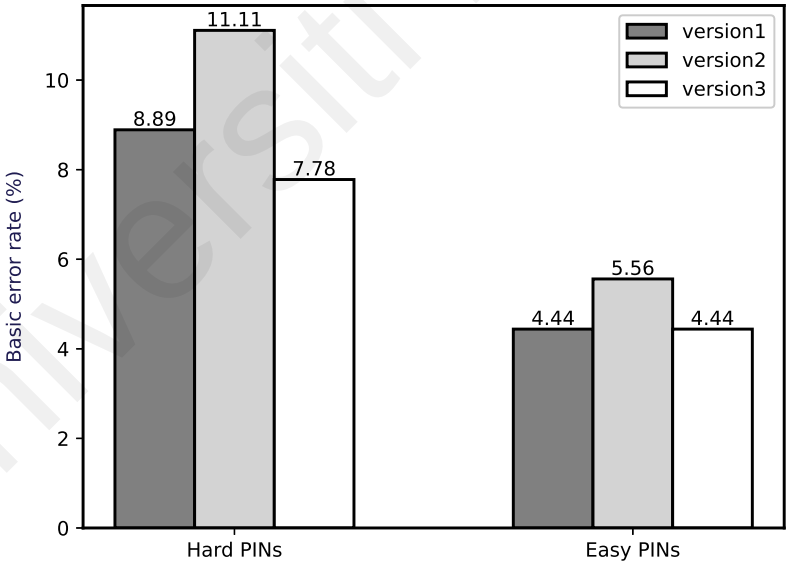


Figure 5.4: Basic error rate for easy and hard PINs of the proposed PIN entry method versions

CHAPTER 6: PRIMARY USER STUDY

6.1 Introduction

The chapter presents the primary user study conducted to evaluate and analyse the security and usability of the proposed PIN-entry method (third version) and compare it against the regular PIN and related work. The security analysis of the proposed PIN-entry method was performed through its resistance to shoulder-surfing, video-based recording, spyware-based recording, and guessing attacks, in addition to a custom scenario of PIN length and challenge digits distribution. The usability analysis of the proposed PIN-entry method was measured using PIN-entry time, error rate, and learning effect. This chapter also describes the questionnaire undertaken to report the user feedback in terms of ease of use, usage, and security. The comparison with related work is presented at the end of this chapter.

6.2 Experimental Settings

A 2x2 within-subject design study was conducted to evaluate the security and usability of the proposed PIN-entry method. The independent variables are PIN type (easy and hard) and PIN method (proposed and regular). The order of the conditions was counterbalanced to reduce the learning effect. Participants were given three attempts per authentication session. A 4-digit PIN is proposed to keep our method simple.

6.2.1 Participants and Procedure

The same thirty participants from the preliminary user study were recruited to conduct this primary study. The procedure was similar to the preliminary user study; it was conducted in three phases: training, testing, and feedback. There was a change in the testing phase regarding the number of times a participants enters his or her PIN. Each participant was asked to enter his or her PIN 10 times instead of three in order to study

the learning effect of the PIN-entry time over longer trials. In the feedback phase, the participants were asked to fill in a questionnaire regarding the ease of use, usage, and security of proposed PIN-entry method.

6.3 Security Analysis

This section analyses the security of the proposed PIN-entry method against shoulder-surfing, video-based recording, spyware-based recording, and guessing attacks, in addition to a custom scenario of PIN length and challenge digits distribution. The shoulder-surfing and recording attack results of the proposed PIN-entry method were reported in the preliminary user study. For the regular PIN, the results show that the regular PIN-entry method is vulnerable to shoulder-surfing attacks because users directly reveal their PINs without any means of protection. So, the attackers did not perform further testing on other attacks (i.e., video-based and spyware-based recordings) for the regular PIN because they succeeded to recover all the participants' PINs through the shoulder-surfing attacks.

6.3.1 Shoulder-surfing Attack

The attackers failed to recover all hard and most easy PINs entered through the proposed PIN-entry method, as shown in Figure 6.1. The proposed PIN-entry method is a type of indirect input method that uses the concept of OTP. That is, an OTP is entered by the user for each authentication session. As a result, the attackers found it difficult to reveal the original PINs even though they captured the OTP. It was also difficult to capture the OTP and the challenge keypad simultaneously. However, they were able to recover 16.67% of the easy PINs. Indeed, all these recovered PINs are composed of four identical digits. Thus, the attackers needed one to three captured authentication sessions to recover these PINs, as shown in Figure 6.2. It was easy for them to recover such PINs as there were only 10 possibilities of the four identical digits, i.e., attackers could narrow down the

possibilities after each trial.

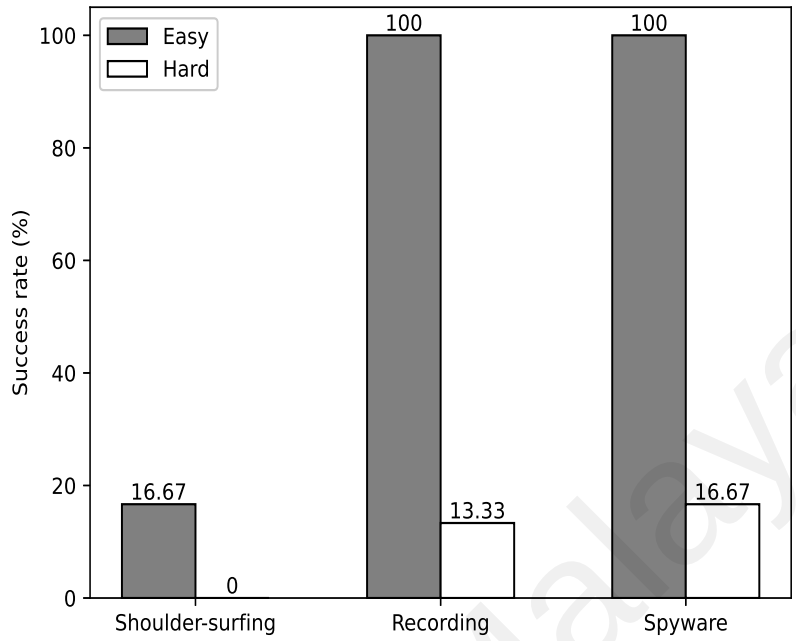


Figure 6.1: Attack success rate for easy and hard PINs of the proposed PIN-entry method.

6.3.2 Video-Based Recording Attack

Video-based recording attacks failed in most hard PIN cases, while they were successful in all cases of easy PINs, as presented in Figure 6.1. The attackers failed to recover most hard PINs because the proposed PIN-entry method produces different, equally likely OTP digits per authentication session. For example, the digit 1 in the OTP could be 1+0, 9+2, 8+3, 7+4, or 6+5 or vice versa.

However, the figure shows that the attackers succeeded in recovering some of the hard PINs entered through the proposed PIN-entry method. In some cases of such PINs, the produced OTP contains two identical digits, according to the R digits distribution. Thus, this helps the attackers predict the pattern of the original PIN and start narrowing down the possibilities. In the other cases, the random distribution of R digits helps the attackers narrow down the possibilities of the PIN digits after each trial. This occurs with the help

of expecting that the first R digits are located at the beginning of the challenge keypad, whereas the last R digits are located at the end of the challenge keypad. The R digits, as we know, are the same PIN digits but ordered according to the key locations of the PIN digits on the regular keypad layout (i.e., 1, 2, 3, ..., 9, 0). Thus, the attackers could narrow down the possibilities of the PIN digits over the trials based on the recorded OTPs and the expected R digits.

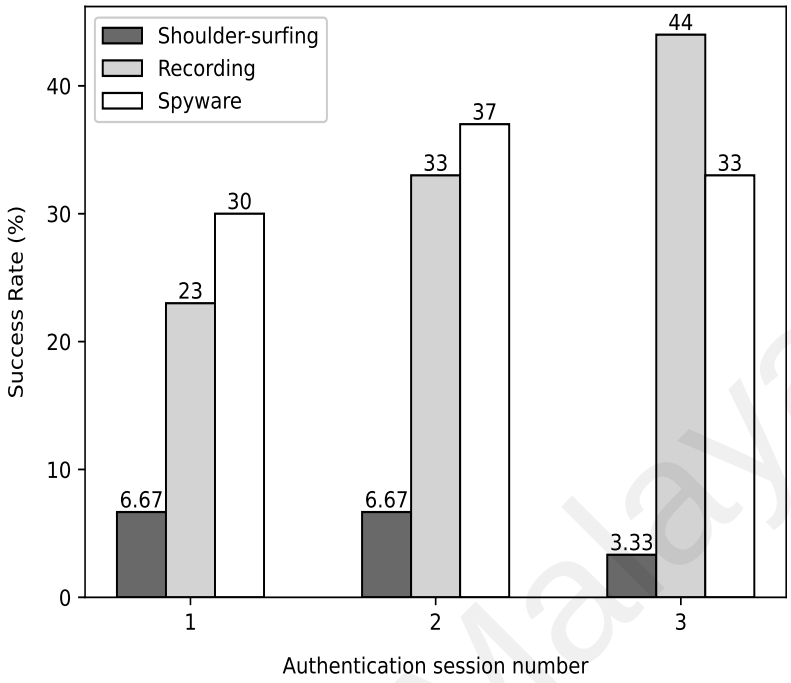
For easy PINs, the attackers succeeded in recovering all the participants' PINs because the produced OTP pattern helped them predict the PIN pattern. In fact, all easy PINs (except for the four-identical digits) are composed of only two distinct digits. Therefore, the produced OTP is always composed of two distinct digits. Hence, attackers need only to assume the correct pair that matches all OTP digits to recover the participant's PIN with the help of the recorded challenge keypad.

Remarkably, the attackers failed to detect all easy PINs and any hard PINs from the first recorded authentication session, as illustrated in Figure 6.2. The figure shows that attackers needed three recorded authentication sessions to recover all easy PINs and some hard PINs. This implies a positive correlation between the number of recorded sessions analysed by the attackers and the attack success rate. It is noteworthy to mention that despite the difficulty of recording the authentication session multiple times, the attackers failed to recover most of the hard PINs entered through the proposed PIN-entry method.

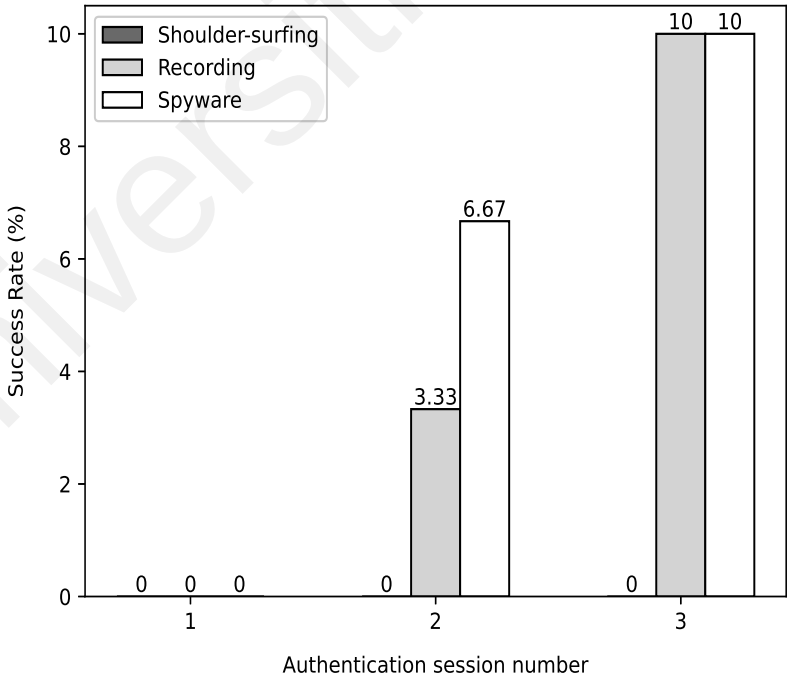
6.3.3 Spyware-Based Recording Attack

Like resisting video-recording attacks, Figure 6.1 shows that spyware attackers succeeded in recovering all easy PINs because the produced OTP pattern reveals the participant's PIN's pattern. The attackers, however, failed to recover most hard PINs due to the difficulty of identifying the PIN's pattern or digits. Similar to video-recording attacks, Figure 6.2 shows that the attackers needed more than one captured session to recover all easy PINs

and some hard PINs.



(a) Easy PINs



(b) Hard PINs

Figure 6.2: Success rate of shoulder-surfing, video-recording, and spyware attacks over three captured authentication sessions

6.3.4 Guessing Attack

A guessing attack is an attempt to login with the most common PINs (dictionary attack) or every possible PIN combinations (brute-force attack). The purpose of analysing the guessing attack is to measure the security level of the proposed PIN-entry method when an attacker has no knowledge of it. To evaluate the proposed PIN-entry method against this attack, we need to compute the PIN space ($digit\ space^{PIN\ length}$). Since the proposed PIN-entry method is the same as the regular 4-digit PIN, the possible PIN combinations are 10^4 (10000). The success probability of both guessing attacks (brute force attack or dictionary) is too low ($\frac{1}{10000}$). However, an attacker may repeat the same PIN to increase his or her opportunity to login since the PIN is dynamic and just four digits. Mathematically, the probability of matching the user's PIN increases with each trial. This attack can be limited by allowing only three continuous failed login attempts, as in the case of the regular PIN-entry method. Also, we can mathematically point out the success probability of shoulder-surfing and recording attacks against a PIN-entry method as reported in (Bultel et al., 2018; M.-K. Lee, Nam, & Kim, 2016). For a challenge-response method, M.-K. Lee, Nam, and Kim (2016) proved that the success probability of guessing, shoulder-surfing and recording attacks are same ($\frac{1}{10000}$ for a 4-digit PIN) when the adversary has no access to the challenge, and all possible responses are equally likely. To some extent, this is applicable to our proposed PIN-entry method. The concise details to mathematically evaluate the success probability of these attacks against both PIN types of the proposed method are left for future work.

6.3.5 Custom Settings

The previous section shows that the recording attacks (video-based and spyware-based) are successful against some of the hard PINs entered through the proposed PIN-entry method. It is argued that this results from the random distribution of the R digits. That is,

the random distribution of R digits helps the attackers to correlate the OTP digits after each trial to narrow down the PIN digit possibilities. So, a custom setting of R digits distribution was created to test if the proposed PIN-entry method is capable of resisting these attacks. R digits were deliberately distributed in this setting to prevent any correlation between authentication sessions. The attackers were allowed to watch three recorded authentication sessions of 10 hard PINs each. They were allowed three guesses per PIN. The results of this custom setting found that the attacker failed to recover any of the hard PINs due to the equally likely OTP digits. The nonrandom distribution of R digits eliminates the correlation between the authentication sessions and leads to narrowing down the PIN digit possibilities. Therefore, the random distribution of R digits helps the attackers to narrow down the PIN digits over trials.

One limitation of the proposed PIN-entry method is the weak resistance of the easy PINs against video-based and spyware-based attacks. In the user study, the 4-digit PIN was employed to keep the method simple. Therefore, all easy PINs (except for the four-identical digits) are composed of only two distinct digits. As a result, the generated OTP pattern helps the attackers predict the PIN pattern and recover it. So, another custom setting of a 6-digit PIN is created so as to check if the PIN length affects the PIN type security (easy and hard) of the proposed PIN-entry method. The attackers were allowed to watch three recorded authentication sessions followed by three guesses. The results of this custom setting are summarised in Table 6.1. It is noted that the attackers succeeded to recover all PINs: two PINs in one recorded session, eight PINs in two recorded sessions, and two PINs in three recorded sessions. The proposed PIN-entry method requires attackers to assume the correct pair(s) (PIN digit(s), challenge digit(s)) that matches all OTP digits in order to recover the victim's PIN using the recorded challenge keypad. For instance, suppose a user created a PIN of 1123. So, the correct pairs that will help the attackers

to identify the PIN digits are (1,1), (1,2), (1,3), (2,3), and vice versa. Assuming one of these pairs may assist the attacker to know the others over the trials. The probability of assuming the correct pair(s) using the 6-digit PIN is undoubtedly higher than the 4-digit PIN. Thus, the success in recovering two digits (a pair) of the 6-digit PIN can easily help the attacker to narrow down the possibilities and recover the PIN digits. Overall, the attack success rate is positively correlated with the PIN length.

Table 6.1: Recording attacks against 6-digit PINs entered through the proposed PIN-entry method

PIN digits	Pattern	Attack status	No. of required recorded sessions
555555	1 distinct digit	Pass	One
333333	1 distinct digit	Pass	One
449499	2 distinct digit	Pass	Three
991991	2 distinct digit	Pass	Two
770977	3 distinct digit	Pass	Two
128222	3 distinct digit	Pass	Three
019112	4 distinct digit	Pass	Two
832818	4 distinct digit	Pass	Two
953192	5 distinct digit	Pass	Two
665498	5 distinct digit	Pass	Two
152698	6 distinct digit	Pass	Two
380791	6 distinct digit	Pass	Two

6.4 Usability Analysis

Usability is a key factor to consider when designing a secure PIN-entry method. Therefore, this section analyses the relative usability of the proposed PIN-entry method in terms of PIN-entry time, error rate, and learning effect and compares it to the regular PIN-entry method. These metrics are widely used in the literature to evaluate PIN-entry methods (Binbeshr et al., 2020). A paired sample t-test was used to measure the effect of the PIN type and the PIN method. A $p < 0.05$ is used for the statistical significance level.

6.4.1 PIN-Entry Time

Figure 6.3 shows the average PIN-entry time for easy and hard PINs of the proposed and regular PIN-entry methods. We can notice that the average PIN-entry time of the proposed PIN-entry method is significantly longer than the regular one regardless of the PIN type ($p < 0.05$). The longer time of the proposed PIN-entry method results from the OTP derivation. It is also noted that users took less time to enter their easy PINs ($5.56s$) using the proposed PIN-entry method than the hard ones ($8.18s$). This is attributed to the ease of locating and calculating the repeated digits an easy PIN contains. The t-test analysis shows a significant effect of the PIN type (easy and hard) on PIN-entry time ($p = 0.023$). With respect to the regular method, the study results reveal no significant difference between easy and hard PINs on PIN-entry time ($p = 0.73$).

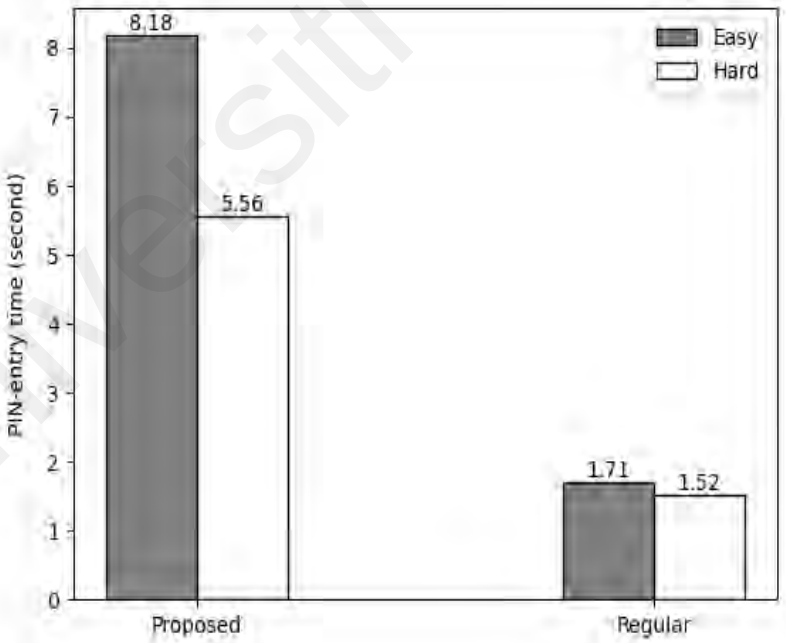


Figure 6.3: PIN-entry time for easy and hard PINs of the proposed and regular PIN-entry methods

6.4.2 Error Rate

Figure 6.4 shows the results of the basic error rate for the easy and hard PINs of the proposed and regular PIN-entry methods. The results show that the proposed PIN-entry method is more error-prone than the regular one for both PIN types. These erroneous login attempts of the proposed PIN-entry method stem from the OTP being derived and entered in one attempt. Nonetheless, participants could perform 10 successful logins in 10 attempts with more than 90%. The t-test results show no significant effects of PIN type on the basic error rate for both PIN-entry methods. For critical error rate, none of the participants failed any authentication session (i.e., all three attempts) for either method.

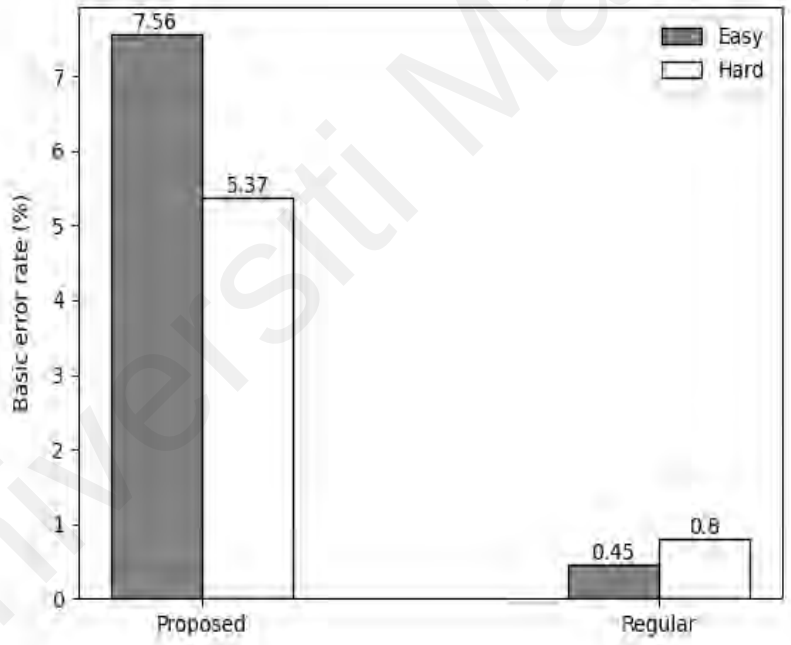


Figure 6.4: Basic error rate for easy and hard PINs of the proposed and regular PIN-entry methods.

6.4.3 Learning Effect

The learning effect was measured among the participants through the variations of the PIN-entry time over 10 trials. Figure 6.5 reveals a learning effect for both types of the proposed PIN-entry method. In particular, the average PIN-entry time decreases

with successive runs. This decrease in PIN-entry time is attributed to the participant's familiarity with the mechanism over time. The average PIN-entry time for both types of regular PIN is relatively stable over time.

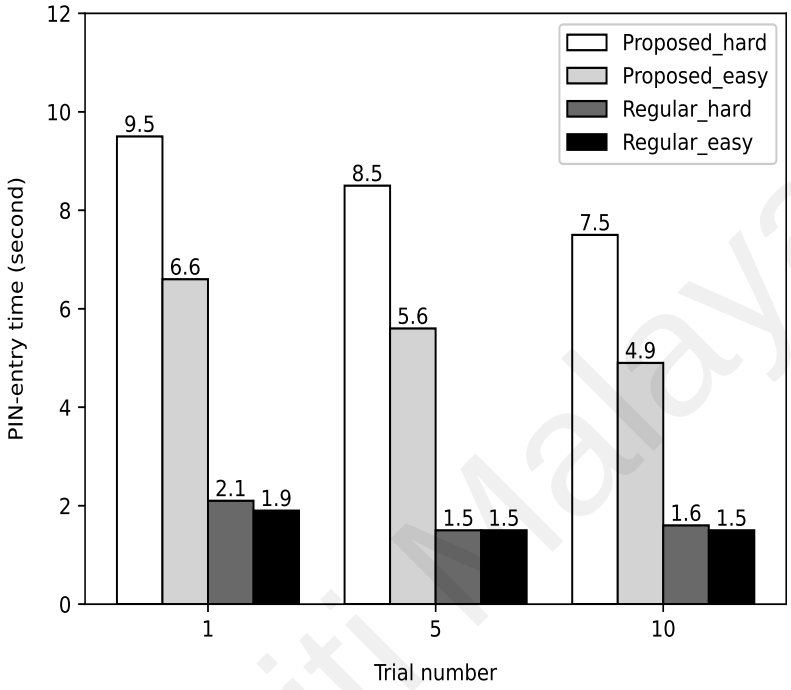


Figure 6.5: Variations in PIN-entry time over 10 trials using easy and hard PINs of the proposed and regular PIN-entry methods.

6.5 User Feedback

Participants were asked to evaluate the proposed PIN-entry method in terms of ease of use, usage, and security through a questionnaire. Figure 6.6 illustrates the questionnaire results using a 5-point Likert scale with a rating from 1 (strongly disagree) to 5 (strongly agree). The use of the 5-point Likert scale is recommended by researchers because it increases the response rate and response quality, in addition to reducing the respondent's frustration (Babakus & Mangold, 1992).

Even though most participants considered that the regular PIN-entry method is more convenient than the proposed one, they agreed that the proposed PIN-entry method is easy to use. This result goes in line with the reported results of the user study regarding

PIN-entry time, error rate, and learning effects in section 6.4. In the case of usage, most participants fully supported the use of the proposed PIN-entry method in critical-security situations, whereas they had different views regarding daily use. This indicates a clear inclination towards the proposed PIN-entry method. For security, all participants perceived the proposed PIN-entry method to resist shoulder-surfing and recording attacks (video-based and spyware-based). They also perceived that the proposed PIN-entry method is more secure than the regular one. This observation supports our previous findings in section 6.3, which show that the proposed PIN-entry method (hard PIN) is secure against such attacks and outperforms the regular PIN-entry method.

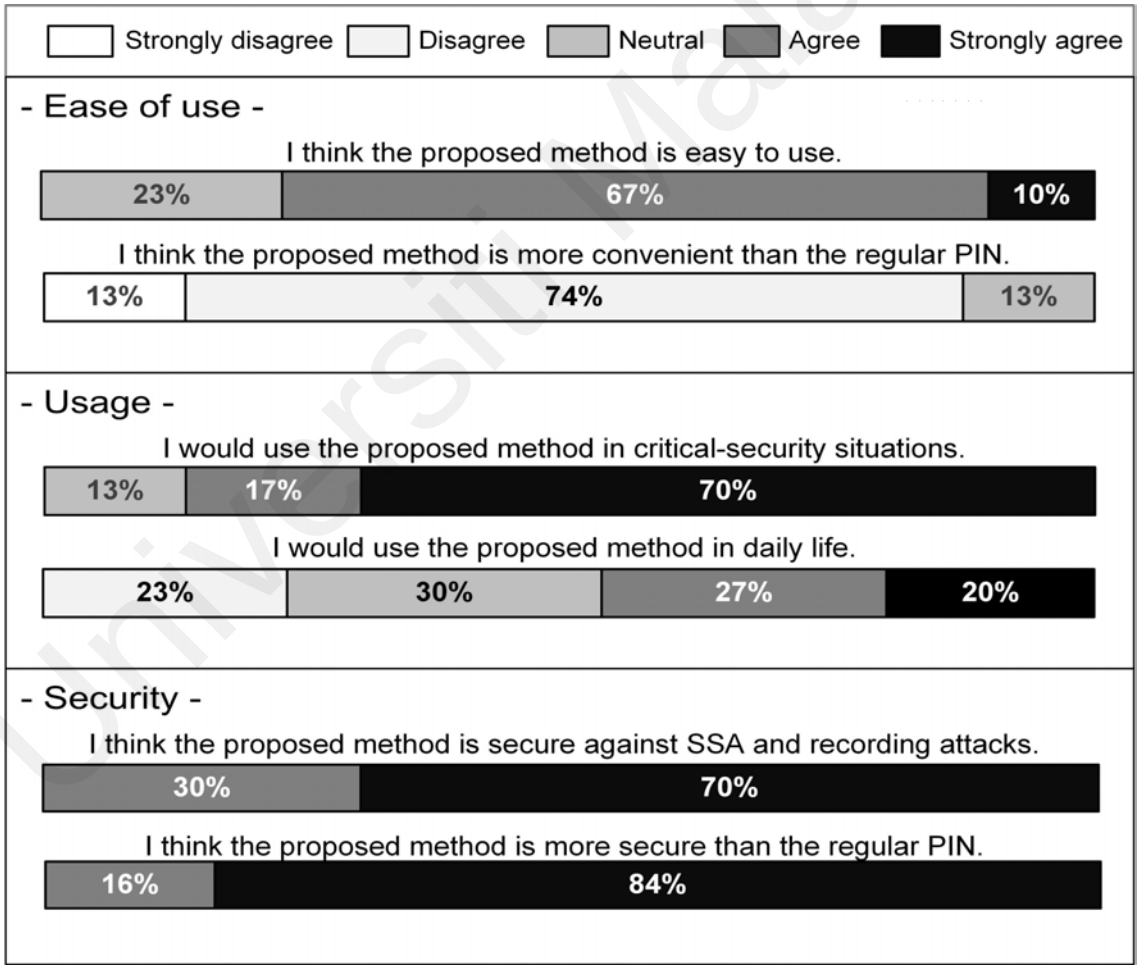


Figure 6.6: Participants' feedback of the proposed PIN-entry method in terms of ease of use, usage, and security.

6.6 Comparison With Related Work

Table 6.2 shows a security and usability comparison of our proposed PIN-entry method with the regular PIN, LIN_4 (M.-K. Lee, 2014), SteganoPIN (Kwon & Na, 2015), and TTU (Nyang et al., 2018). The proposed PIN-entry method was compared with the regular 4-digit PIN-entry method because it is still in use for most forms of user authentication. The other PIN-entry methods are the most relevant and best performing PIN-entry methods in terms of security and usability that employ the concept of OTP (Binbeshr et al., 2020). The level of resistance against attacks has been categorised into vulnerable (not resistant to any attack session), low (resistant to a single session), moderate (partially resistant), and high (fully resistant), as described in Table 6.3.

Table 6.2: Comparison of PIN-entry Methods

PIN-entry Method	Security				Usability		
	SSA	Recording	Spyware	Guessing	PIN-entry Method	Error (basic)	Error (critical)
Regular	Vulnerable	Vulnerable	Vulnerable	$\frac{1}{10^4}$	1.62	0.63%	0
LIN_4	Moderate	Low	Low	$\frac{1}{10^3}$	8.9	N/A	0
SteganoPIN	Moderate	Moderate	Vulnerable	$\frac{1}{10^4}$	5.7	1.1%	0
TTU	Moderate	Moderate	Vulnerable	$\frac{1}{10^4}$	10.42	11.95%	9
Proposed (hard)	High	Hard	Hard	$\frac{1}{10^4}$	8.18	7.56%	0

The proposed PIN-entry method (hard) outperforms all other methods in terms of resisting shoulder-surfing, video-recording, and spyware attacks. This is because it forces users to enter an OTP for each authentication session. The employment of the mod 10 addition produces equally likely OTP digits. Besides, the nonrandom distribution of R digits eliminates the correlation between the authentication sessions, which leads to narrowing down the possibilities of the PIN digits. Thus, attackers failed to recover any hard PINs.

It can be seen that StenagnoPIN and TTU are moderately resistant to both shoulder-

Table 6.3: Level of resistance of a PIN-entry method against shoulder-surfing and recording attacks (Binbeshr et al., 2020)

Level of resistance	Criterion
High	Fully resistant to multiple observed/recorded sessions
Moderate	Partially resistant to multiple observed/recorded sessions
Low	Resistant to only single observed/recorded sessions
Vulnerable	Not resistant to any observed/recorded sessions

surfing and video-based recording attacks. Indeed, these methods rely on the physical hand protection of the challenge. Therefore, improper user posture of the mechanism can reveal the PIN. Both StenagnoPIN and TTU are vulnerable to spyware-based recording attacks because these types of attacks cannot be defeated by physical protection. LIN_4 provides a moderate resistance against shoulder-surfing and low resistance against video-based recording and spyware attacks. The problem with this method is the correlation between the authentication sessions. The attacker needs only two captured sessions to identify the session key and then the original PIN. Shoulder-surfers may require multiple sessions to discover the PIN due to the limited cognitive capabilities of humans. The regular PIN-entry method is vulnerable to all three attacks because it does not provide any means of security. The likelihood of a guessing attack is $\frac{1}{10000}$ for all methods except LIN_4, which employs the first digit of the PIN to identify the session key. Regarding usability, the regular PIN-entry method outperforms all other methods due to the direct input of the PIN. Nonetheless, all methods except TTU match the condition of the secure human executable protocol in which users perform authentication within 10 seconds with at least a 90% success rate.

6.7 Chapter Summary

This chapter discusses the primary study that was used to evaluate and analyse the security and usability of the proposed PIN-entry method (i.e., third version) and compares it against the regular PIN. The proposed PIN-entry method's security was assessed through

its resistance to shoulder-surfing, recording (video-based and spyware-based), and guessing attacks. The primary user study shows that the proposed PIN-entry method with the hard PIN type is immune against shoulder-surfing and recording attacks (video-based and spyware-based) because of the employment of the OTP. On the contrary, the proposed PIN-entry method with the easy PIN type provides only weak resistance against the recording attacks due to the limited number of distinct digits an easy PIN contains. The success probability of guessing attacks against the proposed PIN-entry method is too low. To provide a more in-depth security analysis, custom settings of PIN length and challenge digit distribution were created. The results of the custom settings illustrate that the random distribution of R digits assists attackers in narrowing down the PIN digits over trials, and the attack success rate is positively correlated with the PIN length. The PIN-entry time, error rate, and learning effect analysis show that the proposed PIN-entry method maintains an acceptable level of usability. This chapter also describes the questionnaire undertaken to report the participants' perceptions towards the proposed PIN-entry method in terms of ease of use, usage, and security. Most participants reported that the proposed PIN-entry method was easy to use and fully supported its usage for critical-security situations. All of them perceived that it is more secure than the regular PIN, in addition to its capability of resisting shoulder-surfing and recording attacks. This chapter ends by comparing the proposed PIN-entry method with related work. It is found that the proposed PIN-entry method provides better security than all other methods while maintaining an acceptable level of usability.

CHAPTER 7: CONCLUSION

This chapter discusses the research objectives achieved in this work. Besides, it highlights the main contributions, describes the limitations, and provides areas for future research.

7.1 Objectives

This research work has achieved the following objectives:

1. To review the existent PIN-entry authentication methods that are resistant to shoulder-surfing and recording attacks.
2. To propose a PIN-entry method that resists shoulder-surfing and recording attacks.
3. To develop a prototype of the proposed PIN-entry method.
4. To evaluate the effectiveness of the proposed PIN-entry method in terms of resisting shoulder-surfing and recording attacks using quantitative/qualitative to measure.

To achieve the first objective, a SLR has been conducted to review the existent PIN-entry methods resistant to shoulder-surfing and recording attacks. The SLR evolved through three phases: planning, conducting, and reporting. In the planning phase, a review protocol was developed. It includes eligibility criteria, information sources, search strategy, study selection, quality assessment process, and data extraction strategy. The actual review of the literature was done in the conducting phase. That is, the search string was applied to the identified databases in order to return the relevant research articles. These returned articles were first checked for duplication, and then they were filtered according to the inclusion and exclusion criteria. The irrelevant research articles were removed. The reporting phase involves reporting the results of this SLR. This SLR presents a taxonomy of the PIN-entry methods. It also discussed the research methods and evaluation metrics that were used to evaluate these PIN-entry methods. Besides, it identifies the main challenges that impede

their acceptance and adoption and provides a pledge to conduct further research activities appropriately.

A PIN-entry method that is resistant to shoulder-surfing and recording (video-based and spyware-based) attacks has been proposed to achieve the second goal. The proposed PIN-entry method employs an indirect input method of entering the PIN using the challenge-response approach. In other words, a user is presented with a challenge and is required to compute and enter an OTP based on his or her knowledge of the challenge and the original PIN. The proposed PIN-entry method combines the addition mod 10 with a challenge keypad to generate a OTP password that obscures the original PIN. The use of addition mod 10 generates equally likely OTP digits, removing any correlation between authentication sessions, and thereby resisting shoulder-surfing and recording attacks. The challenge keypad is a miniature random digit keypad that is used to find the challenge digits. It is delivered using the same visual channel that is used to deliver the response. The challenge digits are identified by knowing the PIN digits. Three versions of the proposed PIN-entry method have been designed. Each version employs the addition mod 10 in a different way with respect to producing the OTP.

To achieve the third goal, prototypes of the regular PIN and each version of the proposed PIN-entry method were created for testing and evaluation. To illustrate how a user interacts with these PIN-entry methods, a use case diagram was created. The Python programming language and SQLite were then used to turn these PIN entry methods into functional prototypes. The registration and login processes were modeled using the Python programming language. The developed methods made use of SQLite as a database.

The proposed PIN-entry method was evaluated and analysed using two user studies, preliminary and primary, to achieve the fourth objective. A preliminary user study was carried out in order to determine the best version of the proposed PIN-entry method

in terms of security, usability, and user perception. The third version of the proposed PIN-entry method was chosen for the primary user study, where it was evaluated and compared to the regular PIN method and related work. The user research was divided into three stages: training, testing, and feedback. The training stage began with an explanation of the study's purpose as well as the procedures and task scenarios for each PIN-entry method. Following that, participants received free training until they were ready to take the test. Participants and attackers were asked to enter their PINs (hard and easy) and observe the authentication sessions during the testing stage. Participants were interviewed about which versions they preferred and why (in the preliminary user study) during the feedback stage, and they were asked to fill out a questionnaire (in the primary user study).

7.2 Contributions

The main contributions of this research work are as follows:

- A SLR has been conducted to review the existent PIN-entry methods resistant to shoulder-surfing and recording attacks. This SLR presents a taxonomy of PIN-entry methods resistant to shoulder-surfing and recording attacks. It also discussed the research methods and evaluation metrics used to evaluate these PIN-entry methods. In addition, it identifies the main challenges that impede their acceptance and adoption and provides a pledge to appropriately conduct further research activities. This SLR would be valuable to researchers and practitioners interested in exploring and developing secure and usable PIN-entry methods.
- A usable and compatible PIN-entry method resistant to shoulder-surfing and recording attacks was proposed. The proposed PIN-entry method employs an indirect input method that utilizes the addition mod 10 and a mini-challenge keypad in order to produce a OTP password that obscures the original PIN. The employment of the

addition mod 10 produces equally likely OTP digits so as to remove any correlation between authentication sessions, and thus, resist shoulder-surfing and recording attacks. To simplify the login process and maintain the compatibility with regular PIN-entry method, the proposed PIN-entry method uses the same visual channel to transfer the challenge and deliver the response. In addition, no more information is required from the user to memorize except the PIN. It can be said that the proposed PIN-entry method can provide a better alternative to the regular PIN-entry method, particularly for those who expect a high level of security for their services.

- Three versions of the proposed PIN-entry method have been designed, tested, and compared. These versions are different in the way they use the addition mod 10 to produce the OTP. The first version of the proposed PIN-entry method displays the addition mod 10 table as a matrix (rows and columns). To produce the OTP, the user needs to intersect the PIN digits located on the leftmost column with the challenge digits located on the top row. The second version of the proposed PIN-entry method uses the regular keypad layout to display the addition mod 10 table. The user corresponds the challenge digits on the PIN digits' mini keypads to derive the OTP. Apart from displaying the addition mod 10 table, the third version of the proposed PIN-entry method requires simple human computation. The user needs to produce the OTP based on the addition mod 10 formula that takes two parameters, the PIN and the challenge. These versions of the proposed PIN-entry method provide alternative ways for researchers and practitioners to explore and develop secure and usable PIN-entry methods resistant to shoulder-surfing and recording attacks.

7.3 Limitations and Future Directions

The evaluation, analysis, and discussion stated in the previous chapters have validated the achievement of the aim and objectives of this research study - a secure PIN-entry

method resistant to shoulder-surfing, video-based, and spyware-based recording attacks. However, this research study has a number of limitations that need to be considered in future work. This section describes these limitations and provides suggestions for further research activities.

(a) ***Weak resistance of easy PINs***

One limitation of the proposed PIN-entry method is the weak resistance of the easy PINs against recording attacks due to the limited number of distinct digits. In fact, all easy PINs (except the four identical digits) are composed of only two distinct digits. Therefore, the produced OTP is always composed of two distinct digits. Hence, attackers need only to assume the correct pair that matches all OTP digits to recover the victim's PIN with the help of the recorded challenge keypad.

In future work, it may be desirable to develop a PIN checker to help users avoid easy PINs during the registration process. Users shall not register such PINs in order to avoid the threat of shoulder-surfing and recording attacks. The PIN checker needs to identify the PIN pattern in order to determine the PIN type (easy or hard). It is supposed to guide users to register hard PINs so as to avoid the attacks' threat. Examples of hard PINs are four distinct digits (e.g., 2345) and three distinct digits (e.g., 2321 or 2231). In case of a user register an easy PIN, the PIN checker is supposed to recommend a list of hard PINs based on the entered PIN. The recommended hard PINs can be generated by changing one or two digits of the entered PIN. The new digits must not be identical to any other digits of the PIN. Easy PINs include two distinct digits (e.g., 2121 or 2211), three identical digits (e.g., 2221 or 2212), and four identical digits (e.g., 2222).

(b) ***Usability and security trade-off***

Usability and security are two contradictory requirements in designing PIN-entry methods. For example, the secure PIN-entry authentication method may increase the burden on users to key in the PIN. Thus, users tend to use simple and usable PIN-entry authentication method even though it may affect the security. In this research study, the proposed PIN-entry method provides better security than the existing methods using a challenge-response approach. This challenge-response approach requires a simple human computation in order to produce an OTP that obscures the original PIN. Although the proposed PIN-entry method maintains an acceptable level of usability, the requirement of human computation may be unfavourable by some people.

Future studies could fruitfully investigate the effect of human computation requirement on accepting and adopting the proposed PIN-entry method. To do so, the proposed PIN-entry method could be validated on a large and diverse number of participants. It would also be interesting to explore alternative approaches and discuss the trade-off between security and usability.

(c) ***Lack of a standard evaluation framework***

The lack of a standard evaluation framework for the PIN-entry method that is resistant to shoulder-surfing and recording attacks is an obvious limitation raised by the conducted SLR. The findings of the SLR revealed differences in the use of research methods, experiments settings, sample size, and evaluation metrics. For example, the user study was the dominant research method employed by the selected articles to evaluate the security and usability of the proposed PIN-entry methods. However, some articles employed different research methods, such as security and usability analysis, to evaluate security and usability, respectively. Moreover, some articles encompassed a questionnaire, interview, or both with a user study. Differences in the study settings and sample sizes were also presented in

the selected articles. The quality assessment of these articles showed a lack of justification regarding this matter. Besides, different evaluation metrics were employed by different articles. The variety of these measures may cause confusion about the important ones. Also, some of these measures, such as self-reported security, self-reported usability, and feedback, are extremely general and subjective.

A desirable approach for future research is to build a theoretical framework to rigorously evaluate the security and usability of PIN-entry methods. The threat model of shoulder-surfing and recording attacks, as well as the standard security and usability metrics for evaluating a PIN-entry method, should be clearly defined in the framework. The framework should also include information about the research methods, settings, and sample size. Overall, constructing a standard evaluation framework will be an important area for future research and will promote the process of unifying the conducted experiments.

REFERENCES

Adithya, P., Aishwarya, S., Megalai, S., Priyadharshini, S., & Kurinjimalar, R. (2017). Security enhancement in automated teller machine. In *2017 international conference on intelligent computing and control (i2c2)* (pp. 1–5).

Aljaffan, N. M. D. (2017). *Password security and usability: From password checkers to a new framework for user authentication* (Unpublished doctoral dissertation). University of Surrey (United Kingdom).

Almoctar, H., Irani, P., Peysakhovich, V., & Hurter, C. (2018). Path word: A multimodal password entry method for ad-hoc authentication based on digits' shape and smooth pursuit eye movements. In *Proceedings of the 20th acm international conference on multimodal interaction* (pp. 268–277).

Alroobaea, R., & Mayhew, P. J. (2014). How many participants are really enough for usability studies? In *2014 science and information conference* (pp. 48–56).

Alsuhibany, S. A., & Almutairi, S. G. (2016). Making pin and password entry secure against shoulder surfing using camouflage characters. *International Journal of Computer Science and Information Security*, *14*(7), 328.

Anthonio, H., & Kam, Y. H.-S. (2020). A shoulder-surfing resistant colour image-based authentication method using human vision perception with spatial frequency. In *2020 15th international conference for internet technology and secured transactions (icitst)* (pp. 1–5).

Babakus, E., & Mangold, W. G. (1992). Adapting the servqual scale to hospital services: an empirical investigation. *Health services research*, *26*(6), 767.

Biddle, R., Chiasson, S., & Van Oorschot, P. C. (2012). Graphical passwords: Learning from the first twelve years. *ACM Computing Surveys (CSUR)*, *44*(4), 19.

Binbeshr, F., Kiah, M. M., Por, L. Y., & Zaidan, A. A. (2020). A systematic review of pin-entry methods resistant to shoulder-surfing attacks. *computers & security*, 102116.

Breitinger, F., Tully-Doyle, R., & Hassenfeldt, C. (2020). A survey on smartphone user's security choices, awareness and education. *Computers & Security*, *88*, 101647.

Bultel, X., Dreier, J., Giraud, M., Izaute, M., Kheyrkhah, T., Lafourcade, P., . . . Motá, L. (2018). Security analysis and psychological study of authentication methods with pin codes. In *2018 12th international conference on research challenges in information science (rcis)* (pp. 1–11).

Caporusso, N. (2021). An improved pin input method for the visually impaired. In *2021 44th international convention on information, communication and electronic technology (mipro)* (pp. 476–481).

Carneiro, A. T. S., Elmadjian, C. E. L., Gonzales, C., Coutinho, F. L., & Morimoto, C. H. (2019). Pursuitpass: A visual pursuit-based user authentication system. In *2019 32nd sibgrapi conference on graphics, patterns and images (sibgrapi)* (pp. 226–233).

Chakraborty, N., Anand, S. V., Randhawa, G. S., & Mondal, S. (2016). On designing leakage-resilient vibration based authentication techniques. In *2016 ieee trustcom/bigdatase/ispa* (pp. 1875–1881).

Chakraborty, N., Li, J., Mondal, S., Chen, F., & Pan, Y. (2019). On overcoming the identified limitations of a usable pin entry method. *IEEE Access*, *7*, 124366–124378.

Chakraborty, N., & Mondal, S. (2014). Color pass: An intelligent user interface to resist shoulder surfing attack. In *Students' technology symposium (techsym), 2014 ieee* (pp. 13–18).

Dan, Y.-X., & Ku, W.-C. (2017). A simple observation attacks resistant pin-entry scheme employing audios. In *2017 ieee 9th international conference on communication software and networks (iccsn)* (pp. 1410–1413).

Das, I., Das, R., Singh, S., Banerjee, A., Mohiuddin, M. G., & Chowdhury, A. (2020). Design and implementation of eye pupil movement based pin authentication system. In *2020 ieee vlsi device circuit and system (vlsi dcs)* (pp. 1–6).

Davin, J. T., Aviv, A. J., Wolf, F., & Kuber, R. (2017). Baseline measurements of shoulder surfing analysis and comparability for smartphone unlock authentication. In *Proceedings of the 2017 chi conference extended abstracts on human factors in computing systems* (pp. 2496–2503).

De Zheng, J. (2011). A framework for token and biometrics based authentication in computer systems. *JCP*, *6*(6), 1206–1212.

Dhandapani, G., Ferguson, J., & Freeman, E. (2021). Hapticlock: Eyes-free authentication for mobile devices. In *Proceedings of the 2021 international conference on multimodal interaction* (pp. 195–202).

Egele, M., Kruegel, C., Kirda, E., Yin, H., & Song, D. (2007). Dynamic spyware analysis. *USENIX Annual Technical Conference*.

Eiband, M., Khamis, M., Von Zezschwitz, E., Hussmann, H., & Alt, F. (2017). Understanding shoulder surfing in the wild: Stories from users and observers. In *Proceedings of the 2017 chi conference on human factors in computing systems* (pp. 4254–4265).

Greene, K. K., Franklin, J. M., Greene, K. K., & Kelsey, J. (2016). *Measuring the usability and security of permuted passwords on mobile platforms*. US Department of Commerce, National Institute of Standards and Technology.

Guerar, M., Migliardi, M., Palmieri, F., Verderame, L., & Merlo, A. (2019). Securing pin-based authentication in smartwatches with just two gestures. *Concurrency and Computation: Practice and Experience*, e5549.

Gugenheimer, J., De Luca, A., Hess, H., Karg, S., Wolf, D., & Rukzio, E. (2015). Colorsnakes: Using colored decoys to secure authentication in sensitive contexts. In *Proceedings of the 17th international conference on human-computer interaction with mobile devices and services* (pp. 274–283).

Harbach, M., Von Zezschwitz, E., Fichtner, A., De Luca, A., & Smith, M. (2014). {It's} a hard lock life: A field study of smartphone ({Un) Locking} behavior and risk perception. In *10th symposium on usable privacy and security (soups 2014)* (pp. 213–230).

Herley, C., Van Oorschot, P. C., & Patrick, A. S. (2009). Passwords: If we're so smart, why are we still using them? In *International conference on financial cryptography and data security* (pp. 230–237).

Higashiyama, Y., Yanai, N., Okamura, S., & Fujiwara, T. (2015). Revisiting authentication with shoulder-surfing resistance for smartphones. In *2015 third international symposium on computing and networking (candar)* (pp. 89–95).

Hirakawa, Y., Kogure, Y., & Ohzeki, K. (2015). A password authentication method tolerant to video-recording attacks analyzing multiple authentication operations.

International Journal of Computer Science and Electronic Engineering (IJCSEE), *3*(5), 356–360.

Hirakawa, Y., Kurihara, K., & Ohzeki, K. (2017). Borderless interface for user authentication method tolerant against multiple video-recording attacks. In *2017 international conference on computer systems, electronics and control (iccsec)* (pp. 1144–1148).

Holland, A., & Morelli, T. (2018). Dynamic keypad–digit shuffling for secure pin entry in a virtual world. In *International conference on virtual, augmented and mixed reality* (pp. 102–111).

Hopper, N. J., & Blum, M. (2001). Secure human identification protocols. In *International conference on the theory and application of cryptology and information security* (pp. 52–66).

Hutton, B., Salanti, G., Caldwell, D. M., Chaimani, A., Schmid, C. H., Cameron, C., ... others (2015). The prisma extension statement for reporting of systematic reviews incorporating network meta-analyses of health care interventions: checklist and explanations. *Annals of internal medicine*, *162*(11), 777–784.

Ibrahim, D. M., & Ambreen, S. (2019). Gaze touch cross pin: Secure multimodal authentication using gaze and touch pin. *International Journal of Engineering and Advanced Technology (IJEAT)*, *9*(1), 777–781.

Jain, S., Dabola, S., Binjola, S., & Jindal, R. (2021). Alignpin: Indirect pin selection for protection against repeated shoulder surfing. In *2021 11th international conference on cloud computing, data science & engineering (confluence)* (pp. 594–599).

Jeon, I.-S., & Yoon, E.-J. (2015). A simple pin input technique resisting shoulder surfing and smudge attacks. *Contemporary engineering sciences*, *8*, 747-755.

Kabir, M. M., Hasan, N., Tahmid, M. K. H., Ovi, T. A., & Rozario, V. S. (2020). Enhancing smartphone lock security using vibration enabled randomly positioned numbers. In *Proceedings of the international conference on computing advancements* (pp. 1–7).

Kasat, O. K., & Bhadade, U. S. (2018). Revolving flywheel pin entry method to prevent shoulder surfing attacks. In *2018 3rd international conference for convergence in technology (i2ct)* (pp. 1–5).

Kaspersky. (2022, Feb). *What is spyware?* Retrieved from https://www.kaspersky.com/resource-center/threats/spyware

Keele, S., et al. (2007). *Guidelines for performing systematic literature reviews in software engineering* (Tech. Rep.). Technical report, Ver. 2.3 EBSE Technical Report. EBSE.

Khamis, M., Hassib, M., Zezschwitz, E. v., Bulling, A., & Alt, F. (2017). Gazetouchpin: protecting sensitive data on mobile devices using secure multimodal authentication. In *Proceedings of the 19th acm international conference on multimodal interaction* (pp. 446–450).

Khan, H., Hengartner, U., & Vogel, D. (2018). Evaluating attack and defense strategies for smartphone pin shoulder surfing. In *Proceedings of the 2018 chi conference on human factors in computing systems* (p. 164).

Kim, J.-H., Sharma, G., Cardenas, I. S., Prabakar, N., Iyengar, S., et al. (2017). Dynamicpin: A novel approach towards secure atm authentication. In *2017 international conference on computational science and computational intelligence (csci)* (pp. 68–73).

Kim, T., Yi, J. H., & Seo, C. (2014). Spyware resistant smartphone user authentication scheme. *International journal of distributed sensor networks*, *10*(3), 237125.

Kofod-Petersen, A. (2012). How to do a structured literature review in computer science. *Ver. 0.1. October*, *1*.

Konheim, A. G. (2016). Automated teller machines: their history and authentication protocols. *Journal of Cryptographic Engineering*, *6*(1), 1–29.

Krombholz, K., Hupperich, T., & Holz, T. (2016). Use the force: Evaluating force-sensitive authentication for mobile devices. In *Twelfth symposium on usable privacy and security ({SOUPS} 2016)* (pp. 207–219).

Ku, W.-C., Cheng, B.-R., Yeh, Y.-C., & Chang, C.-J. (2016). A simple sector-based textual-graphical password scheme with resistance to login-recording attacks [Journal Article]. *IEICE TRANSACTIONS on Information and Systems*, *99*(2), 529–532.

Ku, W.-C., & Xu, H.-J. (2019). Efficient shoulder surfing resistant pin authentication scheme

based on localized tactile feedback. In *2019 6th ieee international conference on cyber security and cloud computing (cscloud)/2019 5th ieee international conference on edge computing and scalable cloud (edgecom)* (pp. 151–156).

Kumar, C., Akbari, D., Menges, R., MacKenzie, S., & Staab, S. (2019). Touchgazepath: Multimodal interaction with touch and gaze path for secure yet efficient pin entry. In *2019 international conference on multimodal interaction* (pp. 329–338).

Kwon, T., & Hong, J. (2015). Analysis and improvement of a pin-entry method resilient to shoulder-surfing and recording attacks. *IEEE Transactions on Information Forensics and Security*, *2*(10), 278–292.

Kwon, T., & Na, S. (2014). Switchpin: Securing smartphone pin entry with switchable keypads. In *2014 ieee international conference on consumer electronics (icce)* (pp. 23–24).

Kwon, T., & Na, S. (2015). Steganopin: Two-faced human–machine interface for practical enforcement of pin entry security. *IEEE Transactions on Human-Machine Systems*, *46*(1), 143–150.

Kwon, T., Shin, S., & Na, S. (2014). Covert attentional shoulder surfing: Human adversaries are more powerful than expected. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *44*(6), 716–727.

Lazar, J., Feng, J. H., & Hochheiser, H. (2017). *Research methods in human-computer interaction*. Morgan Kaufmann.

Lee, J.-I., Kim, S., Fukumoto, M., & Lee, B. (2017). Reflector: Distance-independent, private pointing on a reflective screen. In *Proceedings of the 30th annual acm symposium on user interface software and technology* (pp. 351–364).

Lee, M., & Nam, H. (2013). Secure and fast pin-entry method for 3d display. *Proceedings of the SECURWARE*, 26–9.

Lee, M.-K. (2014). Security notions and advanced method for human shoulder-surfing resistant pin-entry. *IEEE Transactions on Information Forensics and Security*, *9*(4), 695–708.

Lee, M.-K., Kim, J. B., & Franklin, M. K. (2016). Enhancing the security of personal

identification numbers with three-dimensional displays. *Mobile Information Systems*, *2016*.

Lee, M.-K., & Nam, H. (2013). Secure and usable pin-entry method with shoulder-surfing resistance. In *International conference on human-computer interaction* (pp. 745–748).

Lee, M.-K., Nam, H., & Kim, D. K. (2016). Secure bimodal pin-entry method using audio signals. *Computers & Security*, *56*, 140–150.

Leftheriotis, I. (2013). User authentication in a multi-touch surface: a chord password system. In *Chi'13 extended abstracts on human factors in computing systems* (pp. 1725–1730).

Li, N., Wu, Q., Liu, J., Hu, W., Qin, B., & Wu, W. (2017). Eyesec: A practical shoulder-surfing resistant gaze-based authentication system. In *International conference on information security practice and experience* (pp. 435–453).

Luo, W., Lan, B., Wan, X., Liu, Z., Zeng, Y., & Ma, J. (2020). Feel vibration: Challenge-response mobile authentication with covert channel. In *2020 ieee 20th international conference on communication technology (icct)* (pp. 1089–1096).

Malkin, N., Harbach, M., De Luca, A., & Egelman, S. (2017). The anatomy of smartphone unlocking: Why and how android users around the world lock their phones. *GetMobile: Mobile Computing and Communications*, *20*(3), 42–46.

Miller, G. A. (1956). The magical number seven, plus or minus two: Some limits on our capacity for processing information. *Psychological review*, *63*(2), 81.

Nandhini, G., & Jayanthy, S. (2019). Mobile communication based security for atm pin entry. In *International conference on computer networks and communication technologies* (pp. 453–467).

Nyang, D., Kim, H., Lee, W., Kang, S.-b., Cho, G., Lee, M.-K., & Mohaisen, A. (2018). Two-thumbs-up: Physical protection for pin entry secure against recording attacks. *Computers & Security*, *78*, 1–15.

O'Gorman, L. (2003). Comparing passwords, tokens, and biometrics for user authentication. *Proceedings of the IEEE*, *91*(12), 2021–2040.

Papadopoulos, A., Nguyen, T., Durmus, E., & Memon, N. (2017). Illusionpin: Shoulder-surfing resistant authentication using hybrid images. *IEEE Transactions on Information Forensics and Security*, *12*(12), 2875–2889.

Perković, T., Čagalj, M., & Rakić, N. (2010). Sssl: shoulder surfing safe login. *Journal of Communications Software and Systems*, *6*(2), 65–73.

Perković, T., Čagalj, M., & Saxena, N. (2010). Shoulder-surfing safe login in a partially observable attacker model. In *International conference on financial cryptography and data security* (pp. 351–358).

Programme, C. A. S. (2019). *Casp checklist.* https://casp-uk.net/wp-content/uploads/2018/01/CASP-Qualitative-Checklist-2018.pdf. (Accessed: 2019-09-30)

Rajarajan, S., Kalita, R., Gayatri, T., & Priyadarsini, P. (2018). Spinpad: A secured pin number based user authentication scheme. In *2018 international conference on recent trends in advance computing (icrtac)* (pp. 53–59).

Roth, V., Richter, K., & Freidinger, R. (2004). A pin-entry method resilient against shoulder surfing [Conference Proceedings]. In *Proceedings of the 11th acm conference on computer and communications security* (pp. 236–245). ACM.

Scroxton, A. (2022). *How okta is regaining customer trust after a cyber attack.* https://www.computerweekly.com/news/252524121/How-Okta-is-regaining-customer-trust-after-a-cyber-attack.

Seetharama, M., Paelke, V., & Röcker, C. (2015). Safetypin: Secure pin entry through eye tracking. In *International conference on human aspects of information security, privacy, and trust* (pp. 426–435).

Seo, H., & Kim, H. (2017). Hidden indicator based pin-entry method using audio signals. *Journal of information and communication convergence engineering*, *15*(2), 91–96.

Seo, H., Kim, J., Kim, H., & Liu, Z. (2017). Personal identification number entry for google glass. *Computers & Electrical Engineering*, *63*, 160–167.

Shen, C., Yu, T., Xu, H., Yang, G., & Guan, X. (2016). User practice in password security: An empirical study of real-life passwords in the wild. *Computers & Security*, *61*,

130–141.

Shepard, R. N. (1967). Recognition memory for words, sentences, and pictures. *Journal of Memory and Language*, *6*(1), 156.

Shi, P., Zhu, B., & Youssef, A. (2009). A rotary pin entry scheme resilient to shoulder-surfing. In *2009 international conference for internet technology and secured transactions,(icitst)* (pp. 1–7).

Shi, P. P. (2010). *Methods and techniques to protect against shoulder surfing and phishing attacks* (Unpublished doctoral dissertation). Concordia University.

Six, J. M., & Macefield, R. (2016). How to determine the right number of participants for usability studies. *San Francisco (CA): UXmatters*.

SM, H. K., Pradyumna, G., Aishwarya, B., & Gayathri, C. (2021). Development of personal identification number authorization algorithm using real-time eye tracking & dynamic keypad generation. In *2021 6th international conference for convergence in technology (i2ct)* (pp. 1–6).

Souza, A., Cunha, Í., & B Oliveira, L. (2018). Nomadikey: User authentication for smart devices based on nomadic keys. *International Journal of Network Management*, *28*(1), e1998.

Stamp, M. (2011). *Information security: principles and practice*. John Wiley & Sons.

Still, J. D., & Bell, J. (2018). Incognito: Shoulder-surfing resistant selection method. *Journal of information security and applications*, *40*, 1–8.

Sugumar, V., & Soundararajan, P. (2017). Cursor masquerade: Masking of authentic cursor using random numeric keypad and spurious cursors. In *2017 third international conference on advances in electrical, electronics, information, communication and bio-informatics (aeeicb)* (pp. 80–84).

Suo, X., Zhu, Y., & Owen, G. S. (2005). Graphical passwords: A survey. In *Computer security applications conference, 21st annual* (pp. 10–pp).

Takada, T., & Kokubun, Y. (2014). Mtapin: multi-touch key input enhances security

of pin authentication while keeping usability. *International Journal of Pervasive Computing and Communications*.

Tolosana, R., Vera-Rodriguez, R., & Fierrez, J. (2019). Biotouchpass: Handwritten passwords for touchscreen biometrics. *IEEE Transactions on Mobile Computing*, *19*(7), 1532–1543.

Uellenbeck, S., Hupperich, T., Wolf, C., & Holz, T. (2015). Tactile one-time pad: Leakage-resilient authentication for smartphones. In *International conference on financial cryptography and data security* (pp. 237–253).

Van Nguyen, T., Sae-Bae, N., & Memon, N. (2017). Draw-a-pin: Authentication using finger-drawn pin on touch devices. *computers & security*, *66*, 115–128.

Vijai, K., & Joseph, N. M. (2018). An efficient security key for practical requirement of pin entry protection section authentication. *International Journal of Advance Research, Ideas and Innovations in Technology*, *4*, 544–549.

Vogel, E. K., & Machizawa, M. G. (2004). Neural activity predicts individual differences in visual working memory capacity. *Nature*, *428*(6984), 748–751.

Von Zezschwitz, E., De Luca, A., Brunkow, B., & Hussmann, H. (2015). Swipin: Fast and secure pin-entry on smartphones. In *Proceedings of the 33rd annual acm conference on human factors in computing systems* (pp. 1403–1406).

Wang, D., Gu, Q., Huang, X., & Wang, P. (2017). Understanding human-chosen pins: characteristics, distribution and security. In *Proceedings of the 2017 acm on asia conference on computer and communications security* (pp. 372–385).

Wang, D., He, D., Cheng, H., & Wang, P. (2016). fuzzypsm: A new password strength meter using fuzzy probabilistic context-free grammars. In *Dependable systems and networks (dsn), 2016 46th annual ieee/ifip international conference on* (pp. 595–606).

Watanabe, K., Higuchi, F., Inami, M., & Igarashi, T. (2012). Cursorcamouflage: multiple dummy cursors as a defense against shoulder surfing. In *Siggraph asia 2012 emerging technologies* (pp. 1–2).

Weaver, J., Mock, K., & Hoanca, B. (2011). Gaze-based password authentication through

automatic clustering of gaze points. In *2011 ieee international conference on systems, man, and cybernetics* (pp. 2749–2754).

Xu, H.-J., Ku, W.-C., & Dan, Y.-X. (2016). An observation attacks resistant pin-entry scheme using localized haptic feedback. In *2016 ieee region 10 symposium (tensymp)* (pp. 59–64).

Yadav, D. K., Ionascu, B., Ongole, S. V. K., Roy, A., & Memon, N. (2015). Design and analysis of shoulder surfing resistant pin based authentication mechanisms on google glass. In *International conference on financial cryptography and data security* (pp. 281–297).