A PRESS TOUCH CODE BASED SECURE GRAPHICAL PASSWORD SCHEME FOR SMART DEVICES

MD SAYFULLAH AL NOMAN RANAK

Master of Science

UNIVERSITI MALAYSIA PAHANG

UNIVERSITI MALAYSIA PAHANG

DECLARATION OF THESIS AND COPYRIGHT

Author's Full Name : MD SAYFULLAH AL NOMAN RANAK
Date of Birth : 22nd May 1993
Title : A Press Touch Code Based Secure Graphical Password Scheme For Smart Devices

Academic Session : SEM 2 2017/2018

I declare that this thesis is classified as:

□	CONFIDENTIAL	(Contains confidential information under the Official Secret Act 1997)*
□	RESTRICTED	(Contains restricted information as specified by the organization where research was done)*
☑	OPEN ACCESS	I agree that my thesis to be published as online open access (Full Text)

I acknowledge that Universiti Malaysia Pahang reserve the right as follows:

1. The Thesis is the Property of Universiti Malaysia Pahang
2. The Library of Universiti Malaysia Pahang has the right to make copies for the purpose of research only.
3. The Library has the right to make copies of the thesis for academic exchange.

Certified by:

_______________________ (Student's Signature)

_______________________ (Supervisor's Signature)

____
New IC/Passport Number
Date:

____
Name of Supervisor
Date:

SUPERVISOR's DECLARATION

We hereby declare that we have checked this thesis and in our opinion, this thesis is adequate in terms of scope and quality for the award of the degree of Master of Science

____

(Supervisor's Signature)

Full Name : DR. MD SAIFUL AZAD

Position : SENIOR LECTURER

Date : JULY 2018

____

(Co-supervisor's Signature)

Full Name : DR. ZAFRIL RIZAL BIN M AZMI

Position : SENIOR LECTURER

Date : JULY 2018

STUDENT'S DECLARATION

I hereby declare that the work in this thesis is based on my original work except for quotations and citation which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at Universiti Malaysia Pahang or any other institutions.

____

(Student's Signature)

Full Name : MD SAYFULLAH AL NOMAN RANAK

ID Number : MCC16005

Date : JULY 2018

A PRESS TOUCH CODE BASED SECURE GRAPHICAL PASSWORD SCHEME FOR SMART DEVICES

MD SAYFULLAH AL NOMAN RANAK

Thesis submitted in fulfillment of the requirements
for the award of the degree of
Master of Science

Faculty of Computer Systems and Software Engineering

UNIVERSITI MALAYSIA PAHANG

JULY 2018

ACKNOWLEDGEMENTS

I am grateful and would like to express my sincere gratitude to my supervisor, Dr. Md Saiful Azad, for his emerging ideas, invaluable guidance, continuous encouragement and constant supports in making this research possible. He has always impressed me with his outstanding professional conduct, his strong conviction for science, and his belief that a masters program is only a start of a life-long learning experience. I appreciate his consistent support from the first day I applied to graduate program to these concluding moments. I am truly grateful for his progressive vision about my training in science, his tolerance of my naive mistakes, and his commitment to my future career. I would like to express very special thanks to my co-supervisor, Dr. Zafril Rizal M. Azmi, for his suggestions and co-operations throughout the study. I would also like to place on record, my sincere thank to Prof. Dr. Kamal Z. Zamli, Dean of Faculty Of Computer Systems & Software Engineering (FSKKP), for guideline, continuos encouragement and providing me with all the necessary facilities for the research. I also sincerely thanks him for the time spent for correcting my many mistakes.

I would also like to thank my parents who not only supported me, also funded my study in initial level. Without this support, it would not be easy for me to start the masters course. Many special thanks go to members of SysNet Lab research group for their excellent co-operations, inspirations, and supports during this study.

Next, my appreciations are expressed towards the administrative staffs in the FSKKP, Institute of Postgraduate Studies (IPS) and International Office (IO) for their passionate to handle all forms of official tasks during my master study. The appreciations also go to all members of Bangladeshi community, local and foreign friends in UMP.

Finally, this research work of masters study is funded and supported by Masters Research Scheme (MRS), from IPS, UMP. I would like to thank UMP for funding the research and helping me to concentrate on the study.

ABSTRAK

Dewasa ini, peranti pintar telah digunakan oleh ramai pengguna untuk urusan seharian. Selari dengan kepopularitiannya, ancaman keselamatan juga meningkat pada nisbah yang tinggi menyebabkan banyak serangan telah dicatatkan. Untuk melawan serangan ini, banyak skim pengesahan grafik berasaskan kata laluan telah dicadangkan. Ia boleh dikelaskan secara umum sebagai *skim Drawmetric*, *Skim Locimetrik*, dan *skim Cognometrik*. Walaubagaimanapun, kebanyakan skim ini tidak memfokuskan kepada saiz skrin; sedangkan, peranti pintar hadir dalam pelbagai saiz. Secara khususnya, ia tidak sesuai untuk peranti pintar kecil kerana saiz skrin yang kecil dan / atau kekurangan papan kekunci bersaiz penuh. Di dalam tesis ini, skema pengesahan selamat bebas skrin yang baru telah dicadangkan, dimana ia juga menawarkan pertahanan yang berpatutan terhadap *serangan pelayan bahu*. Selain bebas dari kebergantungan terhadap saiz skrin, ia juga menawarkan daya tahan terhadap serangan *ttsmudge* dan serangan *ttkekerasan*. Dalam skim yang dicadangkan iaitu Tekan Sentuh (TS) — juga dikenali sebagai, Tekan Paksa di Apple MacBook, Apple Watch, telefon Axon ZTE 7; Sentuhan 3D dengan iPhone 6 dan 7; dan sebagainya — diubah menjadi kod baru yang diberi nama Kod Tekan Sentuh (KTS). Tiga varian kod ini telah direka dan dibangunkan, iaitu mono-KTS, multi-KTS, dan multi-KTS bersama Grid, pada Sistem Pengoperasian Android. Satu eksperimen dan satu tinjauan secara komprehensif telah dijalankan untuk menilai keberkesanan skim yang dicadangkan ini. Eksperimen telah dilakukan untuk mengetahui ketahanan sistem terhadap serangan *ttserangan pelayan bahu*. Di samping itu, untuk menentukan kebolehgunaan skim yang dicadangkan, satu tinjauan komprehensif yang melibatkan 105 peserta telah dijalankan. Hasil eksperimen menunjukkan bahawa skim yang dicadangkan menunjukkan daya tahan yang lebih tinggi terhadap serangan *ttserangan pelayan bahu* berbanding skim pengesahan berkaitan yang sedia ada. Sekali lagi, maklum balas positif direkodkan selepas maklumbalas tinjauan dianalisis; dan responden mengakui bahawa skim yang dicadangkan ini mudah digunakan.

ABSTRACT

Currently, smart devices are carried around by a large number of people and become daily companions. In parallel to their popularities, the security threats are also increasing at a greater ratio; therefore, a considerable number of attacks have been noted in the recent past. To resist these attacks, many passwords-based graphical authentication schemes are proposed. They could be broadly classified as *Drawmetric scheme*, *Locimetric scheme*, and *Cognometric scheme*. However, most of these schemes are not screen size independent; whereas, smart devices come in different sizes. Specifically, they are not suitable for miniature smart devices due to the small screen size and/or lack of full sized keyboards. In this thesis, a new screen size independent secure authentication scheme has been proposed, which also offers an affordable defense against *shoulder surfing attack*. Besides the screen size independency it is also offering resilience against *smudge* attack and *brute force* attack. In the proposed scheme, the Press Touch (PT)—also known as, Force Touch in Apples MacBook, Apple Watch, ZTEs Axon 7 phone; 3D Touch with iPhone 6 and 7; and so on—is transformed into a new type of code, named Press Touch Code(PTC). Three variants of it are designed and implemented, namely mono-PTC, multi-PTC, and multi-PTC with Grid, on the Android Operating System. An in lab experiment and a comprehensive survey have been conducted to evaluate the effectiveness of the proposed scheme. The lab experiment has been performed to discover the resilience of the system against the *shoulder surfing* attack. In addition, to determine the usability of the proposed scheme a comprehensive survey involving 105 perticipants has been conducted. The experimental results demonstrate that the proposed scheme offers a higher resilience against *shoulder surfing* attack over the existing related authentication schemes. Again, positive responses founded, after analyzing the survey feedbacks ; and they admit that the proposed scheme is easy to use.

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

PIN	password identification number
VC	Vibration Code
VAP	Vibration And Pattern
NSF	National Science Foundation
NIST	National Institute of Standards and Technology
PST	Press Sensitive Touch
TI	Tiny Image
APL	Android Pattern Lock
VAPC	Vibration and Pattern Code
AN	Alpha Numeric
FFP	Fat Finger Problem
PTC	Press Touch Code
BPNN	Back Propagation Neural Network
FLD	Fisher Linear Discriminate
PT	Press Touch
PL	Pattern Lock
OS	Operating System
PSS	Pressure sensitive Screen
PTFA	Press Touch Finding Algorithm
BDAS	Background Das
QDAS	Qualitative DAS

CHAPTER 1

INTRODUCTION

1.1 Preamble

At present, smart devices are considered as the modern-day's constant companions of human beings. They have become daily convoy and are used by billions of people. Recent enhancements to smart devices and their appealing applications make them desirable to consumers of all ages. Hence, consumers around the globe are embracing them at a greater ratio. In 2014, around 1.75 billion users worldwide own and use smartphones, which are 25% higher than the earlier year (Total, 2014).

In oppose to non-smart devices like mobile phones, which enable users to only talk and text, smartphones provide users a variety of functionalities, for example, connection to the Internet, online shopping, e-mail and social media, data storage, global positioning systems, and many other applications (Chang, Chen, & Zhou, 2009). Again the latest smart watches not only enable users to monitor times, but also provide functionalities to connect to smartphones and get control over the phones, like reading messages, receiving calls, and sending data. People rely on them with both private and sensitive data, and they store their private information, such as contact details, essential documents, secret and public images, PIN numbers, and other valuable data in their devices for frequent access. These are some of the reasons for the sudden high growth of the smart device consumption. But along with the rapid growth of their usages, assuring information security has become one of the main challenges that researchers and information-security specialists must consider. Even though the smart devices are filled with useful and exciting features, implementing a security infrastructure with them is critical. These devices are vulnerable to various attacks. The primary reason of attacking these devices is to acquire data. In the recent past, a considerable number of attacks have been noticed (Snell, 2016), which lead to undermining accounts, leaked private information, and potential losses for individuals or organizations. Therefore, ensuring security of these devices become a burning issue; and hence, many smart devices employ one or more authentication schemes. In this thesis a new authentication scheme is proposed to tackle several issues of the current authentication scheme, which are detailed below.

1.2 Research Background

The concept of authentication was initiated back in the ancient time of roman military. According to the historian polybius from 118 BCE McGing (2010), a careful procedure for circulating daily signature or 'watchwords' was developed to prevent infiltration. It also exists in folklore, in the tale of Ali Baba and the forty thieves (first translated into English in 1785) (Lane & Poole, 1883). Among various authentication schemes, *password-based* authentication schemes are the most common type of schemes that are utilized on many smart devices due to their lower computational complexities, lower processing requirements, and so forth. However, the tiny screen size of the smart devices compel some constraints in text-based password scheme, as example, limited length password, small on-screen keyboard. Due to the latter constraint, typing turn out to be less precise and inefficient. Consequently, people use even smaller passwords, which make them additionally vulnerable. Again, *text-based* authentication schemes are more common than other existing *password-based* schemes. Several cryptanalysts discovered various vulnerabilities in *text-based* schemes, as example, *dictionary attack* (Pinkas & Sander, 2002), *social engineering* attack (Janczewski & Fu, 2010), *brute force* attack (Owens & Matthews, 2008), *guessing* attack (Goyal, Kumar, Singh, Abraham, & Sanyal, 2005). However in smart devices, *graphical password* schemes are preferred due to several reasons, such as *i*) these schemes are heavily graphic oriented in nature, *ii*) memorability of these schemes are higher over *text-based* schemes in several psychological studies, it has been identified that humans can remember images more than their counterparts, *iii*) these schemes offer a larger password space compare to *text-based* schemes, and so on. Again, in many miniature smart devices—such as smart watch, smart band, and so forth—this type of passwords are not suitable due to unavailability of full/partial keyboards. Hence, most of them are not screen size independent. On the other hand, *graphical password* schemes are also vulnerable to several attacks, like, *shoulder surfing* attack (Lashkari, Farmand, et al., 2009), *smudge* attack (Kwon & Na, 2014), *brute force* attack, and so on. Moreover, they also experience some serious problems, such as *fat finger* problem (De Luca et al., 2013), *tiny image problem*(Suo, Zhu, & Owen, 2005), and so forth. All these attacks and problems leads to the following problem statement.

1.3 Problem Statement

Smart devices come in deifferent sizes; however, most of the existing authention schemes are not screen size independent. More specifically, in many miniature smart devices—such as smart watch, smart band, and so forth—this type of passwords are not suitable due to unavailability of full/partial keyboards. For instance, the tiny screen size of those smart devices imposes some constraints in *text-based* schemes, like, limited length password and small on-screen keyboard. Due to the latter constraint, typing turn out to be less precise and inefficient. Consequently, people use even smaller passwords, which make them additionally vulnerable.

Again, *graphical password* also experience some serious problems, such as *fat finger problem* (De Luca et al., 2013), *tiny image problem*, and so forth. In *fat finger problem*, a user has difficulty in using a touchscreen device because the fields or buttons of the applications are too small for the width of the finger. *Android pattern lock* (Uellenbeck, Dürmuth, Wolf, & Holz, 2013), *tiny lock* (Kwon & Na, 2014), *pass-go* (L. Y. Por, Lim, Su, & Kianoush, 2008), and other resembling schemes suffer from this problem. It is even prominent in miniature smart devices for their limited screen sizes. On the other hand, the *tiny image problem* is more common among the image selection based *graphical password* schemes (Blonder, 1996; Dhamija & Perrig, 2000; Dirik, Memon, & Birget, 2007). It is eminent in the devices with limited screen size. Therefore, alike *text-based* schemes, most of the *graphical password* schemes are also not suitable for the miniature smart devices. In other words, most of them are not screen size independent. Although, smart devices come in different sizes—most of the existing *password-based* authentication schemes are not screen size independent as argued in earlier discussions. Therefore, they fail to ensure the security of all sized smart devices.

Moreover, most of the *password-based* (textual/graphical) authentication schemes are not fully or partialy resistant to many threatening attacks, as example, smudge attack—where an intruder tries to guess the pattern code of the users by tracing the smudges created by them for using the same password in the same screen for a long time (Kwon & Na, 2014); Brute force attack—which is a trial-and-end method used to capture secrete information like password or secret keys by trying every possible combination or guesses (Mihailescu, 2007); shoulder surfing attack—where attackers try to guess the password/pattern by secretly observing while the user is giving password/pattern staying nearby user without his concern (Lashkari, Farmand, et al., 2009). Hence, it remains an important issue to investigate.

1.4 Research Questions

After proper investigation, Some static purposes and problem statements are figured out, which are endeavored to solve throughout this thesis. They are mentioned bellow:

- Most of the current graphical authentication schemes are not screen size independent. They are functional upto a certain screen size. They can't work properly or might become useless (left unused) in the miniature smart devices like smart watch, smart band.

- Most of the graphical authentication schemes of smart devices are not resilliance to *shoulder surfing* attack, since users cannot always stay conscious and hide their passwords from the intruders standing nearby. Again, only a few *graphical password* schemes are resilience against the *smudge* attack due to the smudges formed on the screen, which is quite possible to identify. Moreover, most of the graphical authentication schemes are immured from *brute force* attack.

1.5 Research Objectives

The goal of this thesis is to propose a screen size independent and secure authentication scheme. To attain this goal, follwing objectives are needed to be attained.

- To design a novel screen size independent authentication scheme utilizing the *press touch* technique of smart devices that would offer an affordable defense against the *shoulder surfing* attack.

- To enhance the proposed authentication scheme by integrating grid cells into it to attain resilliance against the *smudge* attack and the *brute force* attack.

- To evaluate the proposed authentication schemes with the existing schemes in terms of security, functionality and usability through conducting experiments and surveys.

1.6 Research Scope

- This work proposes a secure screen size independent authentication scheme, which could be applicable only on all *Pressure Sensitive Technique (PST)* enabled smart devices.

- All the variants of the proposed scheme are implemented on the Android based operating system.

- During the evaluation of the proposed scheme, The existing analogous graphical authentication schemes were mostly focused.

- While comparing with the other graphical authentication schemes, some specific attributes are determined as the key parameters for the sack of the comparison, as example, screen size independence, attack resistant capability, password length, and so forth.

1.7 Research process flow

The research process flow employed in completing this research is comprised of several steps, which includes analyzing exsiting graphical authentication schemes; finding specific problems and generating research objective; proposing new authentication scheme(see Figure 1.1). It also contains—implementing proposed scheme, initial testing, *shoulder surfing* attack resilience experiment, usability evaluation survey. At the end, it concludes by stating the limitations of the proposed scheme and possible future works opportunities.

Literature review on existing schemes: This thesis work starts with a deep critical investigation on the existing standard *graphical* authentication schemes, where their performance are analysed and compared with each other to identify their drawbacks and shortcomings. The detail literature review is mentioned in chapter 2.

Problem statements and research objectives: After investigating the existing *graphical* authentication schemes, some major problems are identified, which are mentioned previously in detail(see section 1.4). They could be summarized as, most of the graphical authentication schemes are not screen size independent. Their resilience against several major attacks, for example, *shoulder surfing* attack, *smudge* attack, *brute force* attack is also not upto the satisfactory level. To resolve these issues, certain research objectives are finalized. The main focus of this research is to develope a screen size independent authentication scheme, which can also attain resilience against above mentioned attacks.

Proposing new authentication scheme: In this thesis, a novel authentication scheme is proposed, where press touch of the existing smart devices are transformed into a code, called Press touch code(PTC), which is described in chapter 3 in detail. It is independent of any screen size and also demonstrate an affordable defense against the *shoulder surfing* attack. An enhancement of the proposed scheme by integrating grid cells is also proposed, which is resilient against the *smudge* and the *brute force* attacks. But this enhanced scheme is suitable only for regular sized smart devices.

Implementing proposed schemes: The proposed schemes is implemented on a *PST*(Press Sensitive Touch) enabled Android OS based smart phone, such as, *Huawei P9 Plus*. Three variants of the proposed scheme are designed and implemented, namely mono-PTC, multi-PTC, and multi-PTC with Grid. The implementation is done with Android developement tool using java programming language. The implemented schemes are applicable for all versions of Android sdk. The ide (*integrated development environment*) used in this implementation is *ANDROID STUDIO*. In the implementation, a certain sized area is defined in the screen, where the pressure is sensed. The detailed description of the implementation is given in chapter 3.

Initial testing: In every step of the implementation, a set of testing is performed to confirm that it is going to the right direction. Changes and modifications are made if the performance do not reach to the satisfactory level. This process continues until the performance reaches to an acceptable level.

Shoulder surfing resilience experiment: After finalizing the implementation, an in-lab experiment is performed to discover the resilience of the system against the *shoulder surfing* attack and compares it with the *Knock Code* since it is the closest competitor of the proposed technique. In the experiment, authentication sessions of both proposed scheme and *Knock Code* schemes are recorded using a camera positioned in different distance and differ-

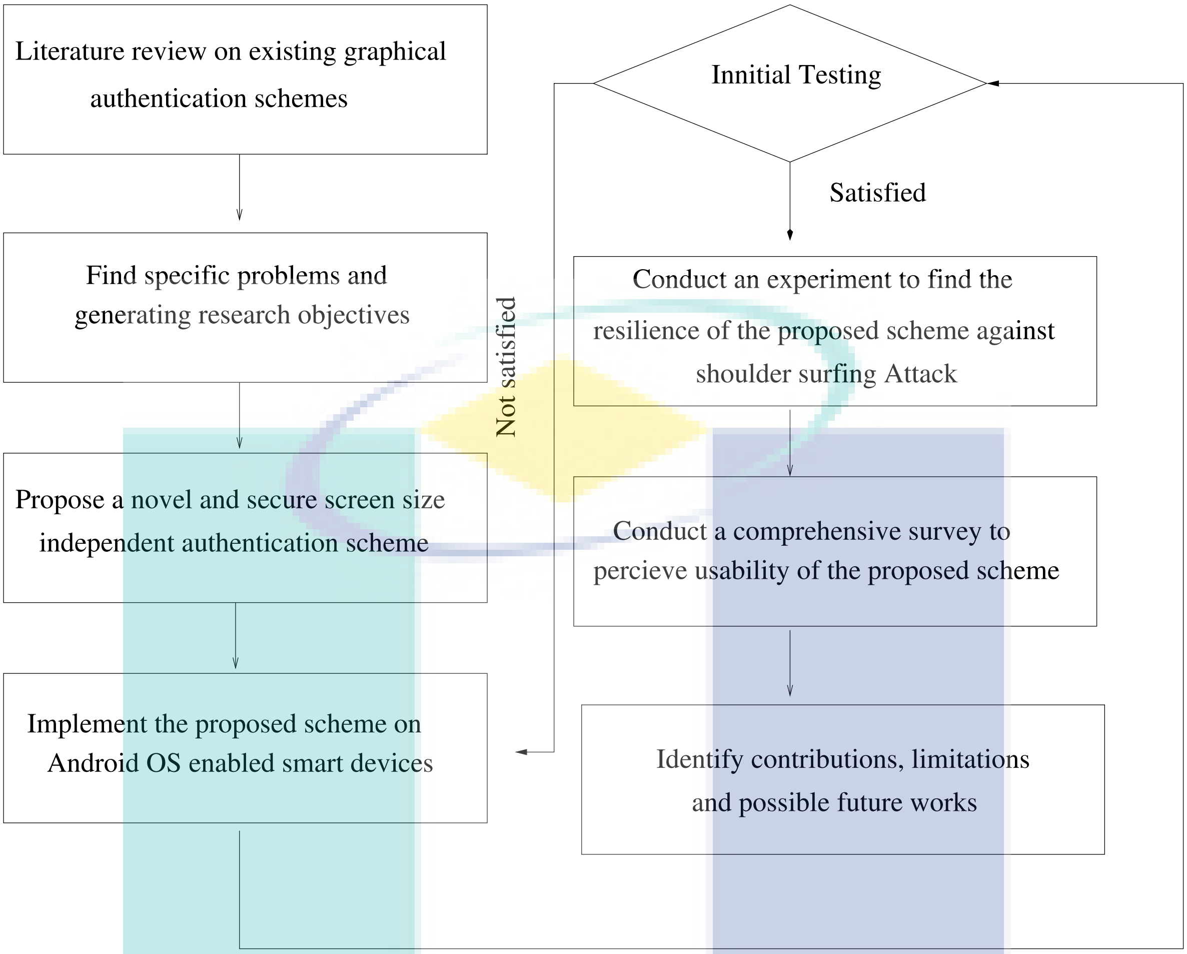
Literature review on existing graphical authentication schemes
Find specific problems and generating research objectives
Propose a novel and secure screen size independent authentication scheme
Implement the proposed scheme on Android OS enabled smart devices
Innitial Testing
Not satisfied
Satisfied
Conduct an experiment to find the resilience of the proposed scheme against shoulder surfing Attack
Conduct a comprehensive survey to percieve usability of the proposed scheme
Identify contributions, limitations and possible future works

Figure 1.1. Research process followed in this thesis

ent height. In every session—irrespective of the scheme—a random signature was registered and it was noted down on a paper for future reference. The recorded videos are played to a number of participants and asked them to find out the signature for all the sessions. The details of this experiment is demonstrated in chapter 3.

Usability evaluation survey: A comprehensive survey on 105 male and female smart phone users of different demographics is also conducted to find out the usability of the proposed scheme. Data is collected through observation of the participants' interaction with the scheme as well as through asking several questions to the participants. After a brief description of the scheme, participants are instructed to first register and then authenticate themselves in the system. After successfully completing the registration and authentication session, the participants are asked various questions to acquire their feedbacks on the proposed scheme. Chapter 3 contains the elaborate discussion of this survey.

Identify Contributions, limitations and possible future works: At the end, contributions of the thesis and limitations of the proposed schemes and its variants are identified. The notable contributions of the thesis are: i) design and implementation of a novel screen size independent authentication scheme; ii) enhancing the proposed scheme by integrating grid cells to offer higher degree of security. The prime limitation of the proposed schemes is that they are only applicable to the *PST* enabled smart devices. Again the mono-PTC and multi-PTC are vulnerable against the *brute force* attack. On the other hand, multi-PTC with Grid is not screen size independent. The future works of this thesis also have been identified and stated at the end of the conclusion.

1.8 Outline of the Thesis

This thesis contains five chapters namely Introduction, Literature Review, Methodology, Results and Discussion and Conclusion.

Chapter 1 introduces the work along with the research background, research statements, problem statement, objectives and research scopes. This chapter portraits a clear motivation/goal behind the current work and the step by step objectives to achieve that goal. It also clarifies where and where not the proposed techniques can be applied and the limitations of them.

Chapter 2 presents the related works, where most of the prominent graphical schemes are detailed with their advantages and limitations. In this process these schemes are keenly analysed and scrutinized, and then the results of the investigation are summarized in the relevant tables. At the end, a critical analysis is performed to demonstrate the possible research direction which leads to the current research that is conducted in this thesis.

In chapter 3, research design and methodology are mentioned, where the proposed technique is detailed along with necessary algorithms. Besides this, the detail of the experimental setup and survey setup are also elaborated in this chapter. Again, all the performance evaluation perameters are also discussed with adequate detail.

Computational results and discussions on evaluating the concept by choosing the different criteria are given in chapter 4. Results of an experimental survey are discussed and indicated a distinct decision based on the results. The survey data set is extracted from a large number of participants who used the proposed technique. These data are being analysed according to the user experience. The validity threats are also discussed, which debates the suitability of utilizing various parameters.

Finally, in chapter 5, the contributions, limitations and conclusion are provided, including the main finding of the work and the outline of the future direction.

CHAPTER 2

LITERATURE REVIEW

2.1 Preamble

A key area in security research is authentication (Blackburn, Miles, Wing, & Shepard, 2007), which is the determination of whether a user should be allowed access to a given system or a resource. In other words, it is the process which determines whether someone or something is, in fact, who or what it is declared to be (Karnan, Akila, & Krishnaraj, 2011). In reality, it is actually the way toward confirming whether any computer or any individual is genuine (Matyas & Stapleton, 2000). It could be again consider as the validation of the identity of a individual who produces some data, and of the identity of the integrity of the data (Neuman & Ts'o, 1994). In a nutshell, authentication is a process or a procedure by which a user tries to get access to a pre-registered system by giving his/her secret credential. On the other hand, authentication schemes are often attacked by the intruders to get access to a system. In this case, the intruders follow certain attacking techniques or procedures to breach the security. Most common attacks on authentication schemes are described in the following section.

2.2 Common Attacks on Authentication scheme

Although, there exist a considerable number of attacks on authentication schemes; however, only related attacks are detailed below.

2.2.1 Shoulder Surfing Attack

An attacker tries to guess target's secrete key by roaming around the target and watch when target is providing password in a system or observe through the camera (Lashkari, Farmand, et al., 2009) (Tari, Ozok, & Holden, 2006).

2.2.2 Smudge Attack

The *smudge* attack is another prominent attack, which is difficult to eliminate. When a user enters a *graphical* password, oily residues or smudges remain on the screen. It is possible to easily determine the password by analyzing these oily smudges. A recent study found that using a variety of lighting angles, light sources, and various camera angles (60 angle for the best output), it is possible to partially unlock a phone in around 92% of cases and fully in around 68% cases (Aviv, Gibson, Mossop, Blaze, & Smith, 2010) (Von Zezschwitz, Koslow, De Luca, & Hussmann, 2013).

2.2.3 Brute Force Attack

Brute force attack is a trial-and-error based method which is used to capture secrete information such as password, Personal Identification Number (PIN) and so on. An automated system generate a large amount of consecutive guesses as to the value of desired data. Brute force attack is used by miscreant to get any secrete data for accessing in a system (Owens & Matthews, 2008) (Ratha, Connell, & Bolle, 2001).

2.2.4 Dictionary Attack

Since large number of the user use password from almost same domain (Morris & Thompson, 1979) (Klein, 1990), that's why human chosen passwords are inherently most insecure. So the miscreant attempt to login/attack in the system with a small number of guesses in this compact domain until they find the real/correct one. This kind of attack is known as *dictionary* attack (Pinkas & Sander, 2002) (Bellare, Pointcheval, & Rogaway, 2000).

2.2.5 Social Engineering-Based Attack

In information security, *social engineering* psychologically manipulate people for disclosing confidential information. It mostly relies on interaction with human and often manipulate target people into breaking security protocol (Janczewski & Fu, 2010) (Krombholz, Hobel, Huber, & Weippl, 2015).

2.2.6 Guessing Attack

Password *guessing* (a.k.a. On-line Password Cracking) is an attack in which an attacker attempts to recover user credentials through the process of attempting to log in repeatedly (Goyal et al., 2005) (Ding & Horster, 1995).

2.2.7 Fat-Finger problem

Due to the *fat finger* problem, sometimes user fall in trouble in giving proper password, and the attackers takes advantages of them (De Luca et al., 2013).

2.3 Classification of authentication schemes

The area of authentication is very wide and enrich. Figure 2.1 shows a comprehensive sight of authentication. As could be observed from the figure, in the context of security, it takes into account TWO (2) primary essential procedures.

1. Elementary Authentication: All authentication schemes that are utilized to access various systems fall under this class. They can be further classified in THREE 3 sub-classes.

(a) *Memorization Based* Authentication, where user have to memorize their secret authentication key.

(b) *Non-memorization Based* Authentication, where user do not need to memorize any secret information. The system will recognize a user by any physical/behavioral attributes or by any token belongs to him/her.

(c) *Hybrid* Authentication, which are the combination of both *memorization* based and *non-memorization based* authentication.

2. *Backup* Authentication: This class of schemes are employed when users forgot their credentials and try to regain them.

Since the proposed scheme is a memorization based authentication scheme(as highlighted in Figure 2.1): hence, follwing discussions only elaborate such schemes.

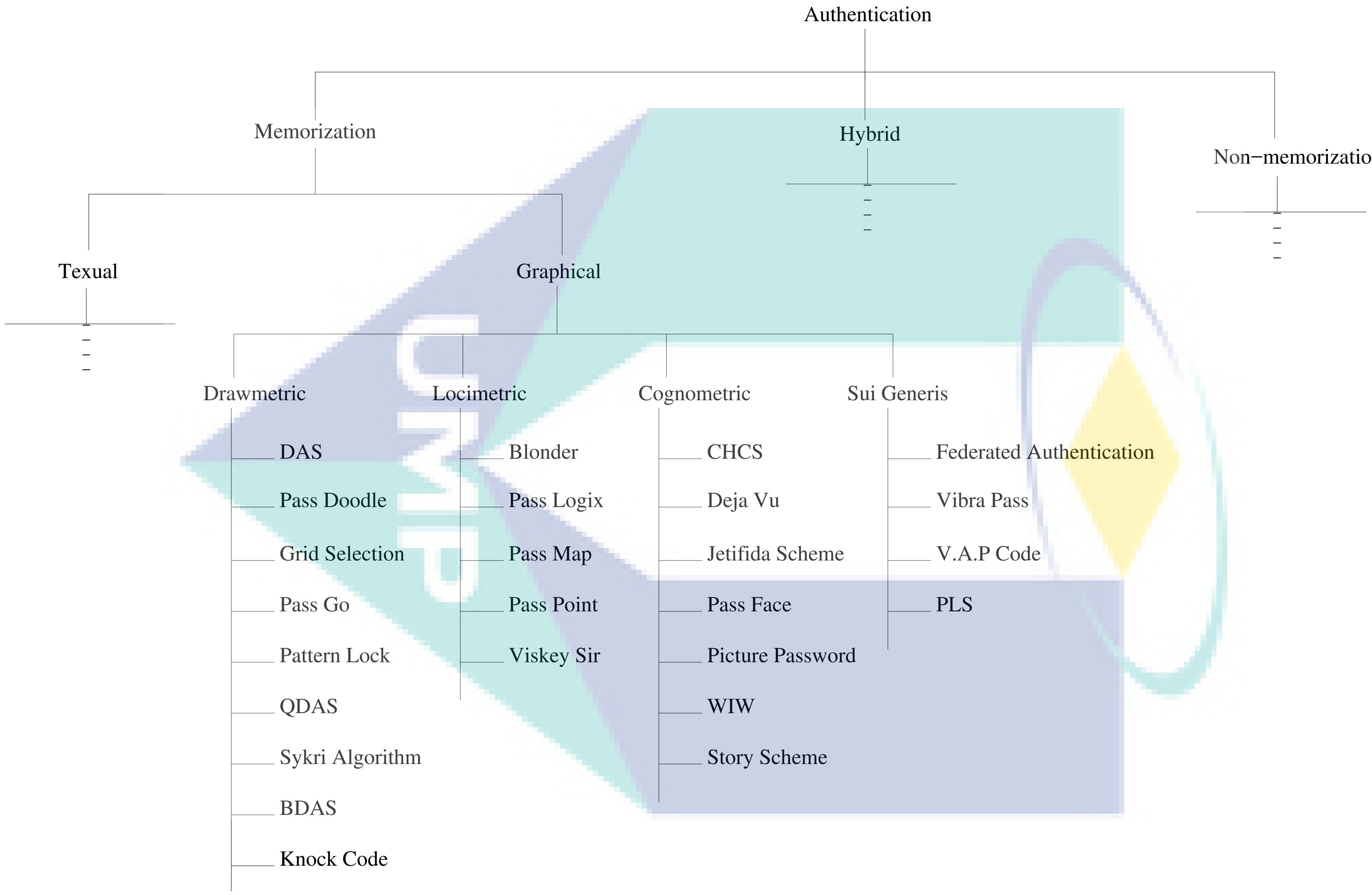

Figure 2.1. A Brief Classification Of Authentication

2.4 Memorization Based Authentication

As discussed earlier, *memorization based* authentication requires user to memorize their secret key. The secret could be *graphical* or *textual*. According to recent study and, The *memorization based* authentication is classified into two different categories.

- *Textual* authentication, where the secret information is only texual.

- *Graphical* authentication, where the secret could be image, diagram or symbol.

An extensive view of *graphical* authentication is discussed in this thesis, as the context that the propose scheme is one of them.

2.4.1 Graphical Authentication

Graphical password was initially presented by Blonder (1996) (Blonder, 1996). His strategy was a couple picked areas of a picture ought to be clicked in by the user with the assistance of mouse or stylus. The user verify if the right district is clicked else he will be rejected (Wiedenbeck, Waters, Birget, Brodskiy, & Memon, 2005b). A *graphical* password is one of a kind sort of password which require tapping on picture instead of writing alphanumeric/numeric string, which essentially came to take care of the issue of secure and vital password (Wiedenbeck et al., 2005b), in light of the fact that reviews has demonstrated that picture is recollected as opposed to password (Dhamija & Perrig, 2000). A *graphical* password key shows a foreordained picture and the requires the user to touch/tap on his predetermined zones as per a foreordained sequence. The password is set by letting the regions to demonstrate the already decided regions, or ”tap locales”, to a user, and requiring the user to touch/click these tap districts in an area and grouping inside the *graphical* picture by which the user coveted password to be set at (Blonder, 1996). *Graphical* secret word system are classified into 3 classification (Gao, Jia, Ye, & Ma, 2013), namely, *Drawmetric* schemes, *Locimetric* schemes, *Cognometrics* schemes.

2.4.1.1 Drawmetric Schemes

Drawmetric schemes are also known as recall-based schemes (De Angeli, Coventry, Johnson, & Renaud, 2005). In *Drawmetric* schemes a user reproduces an outline drawing on a grid that he or she created or selected during the registration stage (Gao et al., 2013). Many *graphical* authentication scheme can fall under *Drawmetric* schemes.

Draw-A-Secret(DAS)

In this technique, a user draws a secret design—that would be utilized as the credential of that user—on a grid of size $N \times N$. Each cell in this grid is denoted by discrete rectangular coordinates (Jermyn et al., 1999), e.g., $C = (x, y) \in (1 :: N) \times (1 :: N)$. When a user draws a design on the grid, the drawing is mapped into a sequence, S of coordinate pairs, C_i, where $i \in \mathbb{Z}^+$, by listing the cells in order through which it passes. This procedure continues until the "pen up" event occurs, i.e., whenever the user lifts the pen from the drawing surface, which is considered as the end of drawing. At the end, S can be represented as $S = C_1, C_2, C_3, ..., C_n$, where $n \in \mathbb{Z}^+$ and $|S| = n$. For instance, consider the drawing given in Figure 2.2, where S generated by this drawing is as follows,

$$S = \{(5,3),(5,2),(4,2),(3,2),(3,3),(3,4),(4,4),(5,4),(5,3),(6,2)\}$$

Here, $(6,2)$ is the end of the drawing where the event "pen up" occurs. If there are a second cycle of drawing in this example, then the new coordinates would be appended to the end of the current sequence. Two drawing would be deemed equivalent if they have the same encoding, i.e., if both of them have crossed the same sequence of grid cells in order. In other words, S and S' would be equivalent if $C_i \in S = C'_i \in S'$ where $i \in \mathbb{Z}^+$, $i \leq |S|, |S'|$.

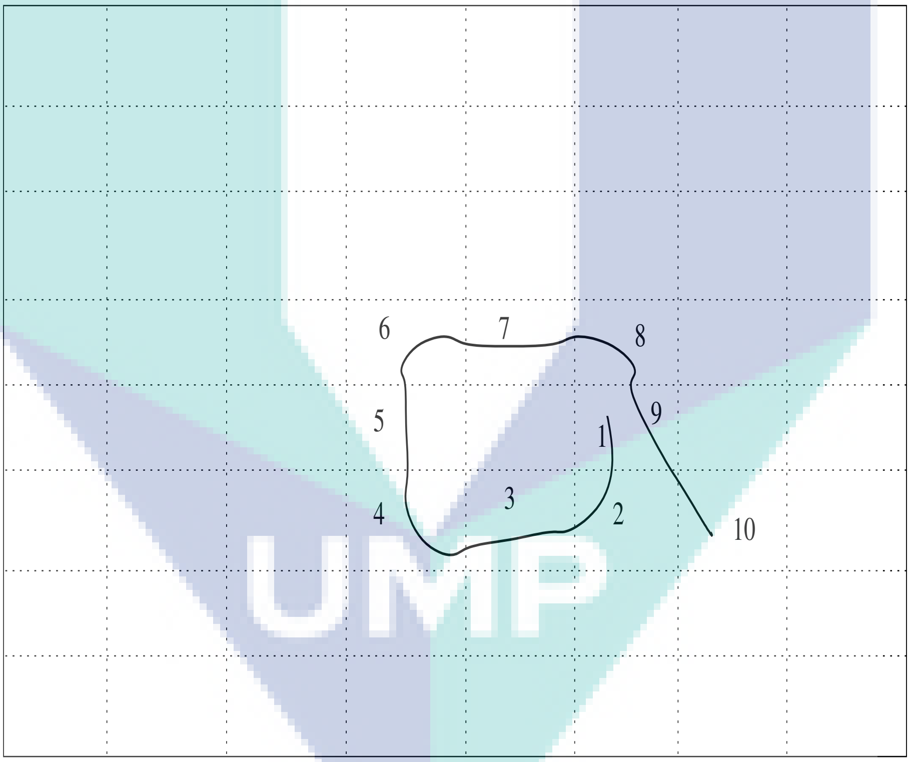

Figure 2.2. Draw-A-Secret (DAS)

One of the main advantages of this approach is that it is alphabet independent; thus, making it equally accessible for speakers of any language. Users are freed from remembering any kind of alphanumeric string. Again, another significant advantage of *DAS* is that a long password could be generated through repeating the drawing cycle multiple times, which is also suggested. Hence, this technique can resist *brute force* attack if a user chooses a long password with many composite strokes. Despite this, it still has many possibilities of getting breached by *dictionary* attack (Thorpe & van Oorschot, 2004) due to choosing mirror symmetric passwords. It has been observed that people recall symmetric images better than asymmetric images; and therefore, the security of the *DAS* scheme may be substantially lower than originally believed (Suo et al., 2005). Again, this scheme is vulnerable to *shoulder surfing* attack since any one picking the phone can memorize the drawing fully or partially.

Grid Selection

When Thorpe and van Oorschot investigated the impact of password length and stroke-count as a complexity property of the *DAS* scheme in 2004, they discovered that stroke-count has the largest impact on its password space. For a fixed password length, the password space decreases significantly with fewer strokes; whereas, the opposite has a lesser impact. Consequently, to improve the security, they proposed *grid selection* technique (Thorpe & van Oorschot, 2004). In this technique, a user is offered a large selection grid cells initially, $G \times G$. Among them, the user has to select a drawing grid cell, which is zoomed in after selection, where the user enters his/her credential as per the original *DAS* scheme (discussed in Section 2.4.1.1). Choosing the location of the drawing grid cell adds an extra degree of complexity in the scheme as the selection has to performed from thousands of possible cells.

In theory, this slight addition to the *DAS* scheme significantly increase the password space, e.g., if a password space, P of *DAS* scheme is ρ; then, it is for the *grid selection* is,

$$P = \frac{G \times G \times \rho}{N \times N}. \tag{2.1}$$

However, to the best of knowledge, there is no user study has been carried out for such *grid selection* technique; so it is unclear whether it works as well in practice as expected. Again, this scheme only enhances the password space of the *DAS* scheme, but the lacks of it still remains.

Pass Go

This scheme (Tao & Adams, 2008) was inspired by a famous ancient Chinese game, named *Go*, which was developed between $3,000$ and $4,000$ years ago. It is an improvement over the original *DAS* scheme and like its predecessor, it is also a grid-based scheme. However, unlike the original *DAS* scheme, in *Pass Go*, a user is required to select or touch on the crossing points rather than the cells. Again, intersections are represented as a matrix as opposed to cells as in its predecessor. Since intersections are points without particular areas, a precise touch on a intersection point is difficult without any error. Therefore, an error tolerance mechanism is employed, and for which, predefined sensitive areas around the intersections—which are invisible to the users—are introduced as depicted in Figure 2.3. Touching any place inside such an area is treated as touching the corresponding intersection point.

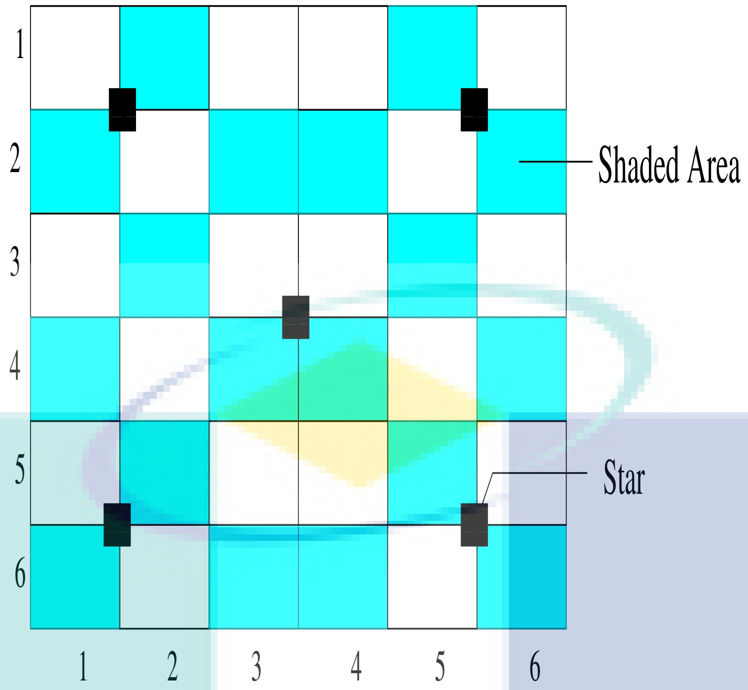

Figure 2.3. Pass Go

The main advantage of changing to intersection points is that drawing diagonal lines are more feasible than its counterpart, and thus, it offers stronger security and better usability (Tao & Adams, 2008). However, alike the original *DAS*, no precaution has been taken to resist the *shoulder surfing* attack. Again, since the sensitive areas are invisible and tiny, it suffers from *fat finger* problem. Moreover, due to the same cause, it is difficult to identify the reason of access denial—which could be overcome by spending a considerable time in practice (L. Por & Lim, 2008).

Pattern Lock

It (Andriotis, Tryfonas, & Oikonomou, 2014) is one of the most popular contemporary authentication schemes that comes integrated with the *Android* mobile operating system. The inspiration of this scheme came from the *pass-go* (described in Section 2.4.1.1) scheme, but the grid size has been reduced to 3×3 as demonstrated in Figure 2.4 to fit it on the standardized size of mobile devices. Mainly, *Pattern Lock* is a line connecting technique with some basic rules, namely *i*) at least four (4) cells must have to select to form a credential, *ii*) a selected node cannot be selected again, and *iii*) jumps across the unselected nodes are prohibited.

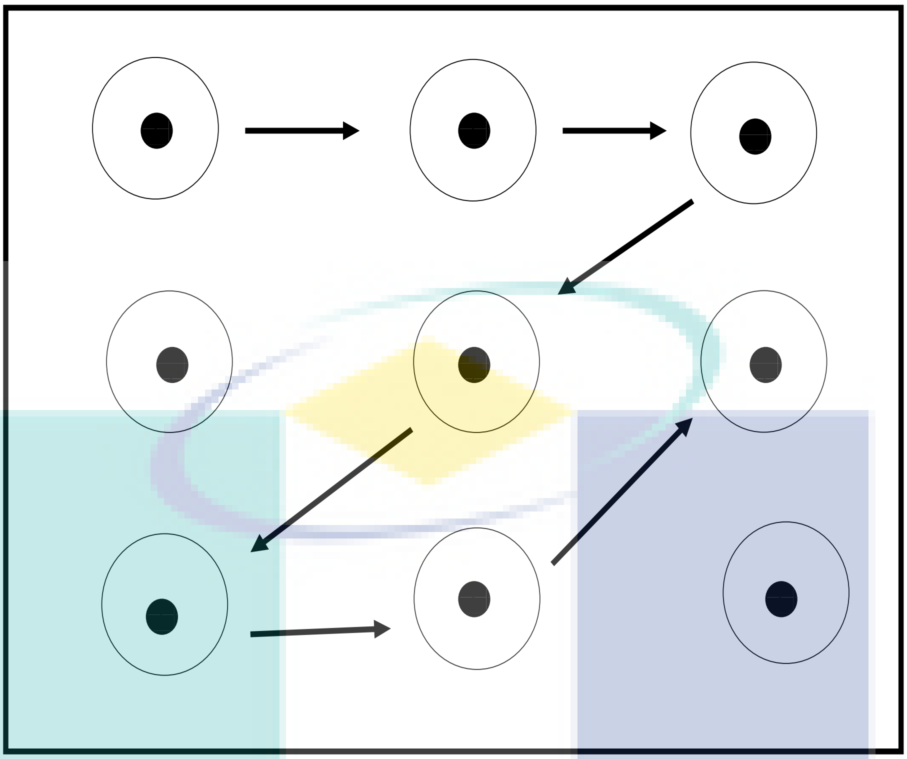

Figure 2.4. Pattern Lock

Although, theoretically it offers 389, 112 unique patterns; however, in reality, due to the restrictions, at most 140, 704 patterns are possible to be drawn (Aviv et al., 2010). Alike its predecessor, it has a limited resilience against the *shoulder surfing* attack. Moreover, the oily residues of the screen create smudges and makes *smudge* attack possible. To attain resilience against the *smudge*, attack *Tiny-lock* scheme—an extension to the original *Pattern Lock*—is proposed in (Kwon & Na, 2014). Unlike its predecessor, the grids in *Tiny-lock* are really tiny, and they are rotatable in clockwise or counter-clockwise direction to complete the process. However, tiny grids impose constraints to the users with weak vision—specifically on mobile devices with small screens, and it also suffers from the *fat-finger* problem.

Qualitative DAS (QDAS)

To tackle the *shoulder surfing* attack of the *DAS* scheme, in *QDAS*, it is extended with two components, namely *i*) qualitative spatial descriptions of strokes and *ii*) dynamic grid transformations. In the former component, the encoding consists of its starting stroke and the sequence of qualitative direction changes, unlike *DAS*. A direction change is assumed when the pen crosses a cell boundary in a direction that is different from the previous cell. For instance, in Figure X, the encoding starts at cell 5, followed by “up”, “right”, and “down”. Unlike *DAS*(2.4.1.1), *QDAS* provides freedom to a user to deviate from the literal spatial definition of their secret. The *QDAS* attains resilience against the *shoulder surfing* attack through employing the latter component, i.e., dynamic grid transformations, which is demonstrated in Figure 2.5. When a user creates a stroke, the most important attributes are the index of the starting cell and the sequence of direction changes before ”pen up” event occurs.

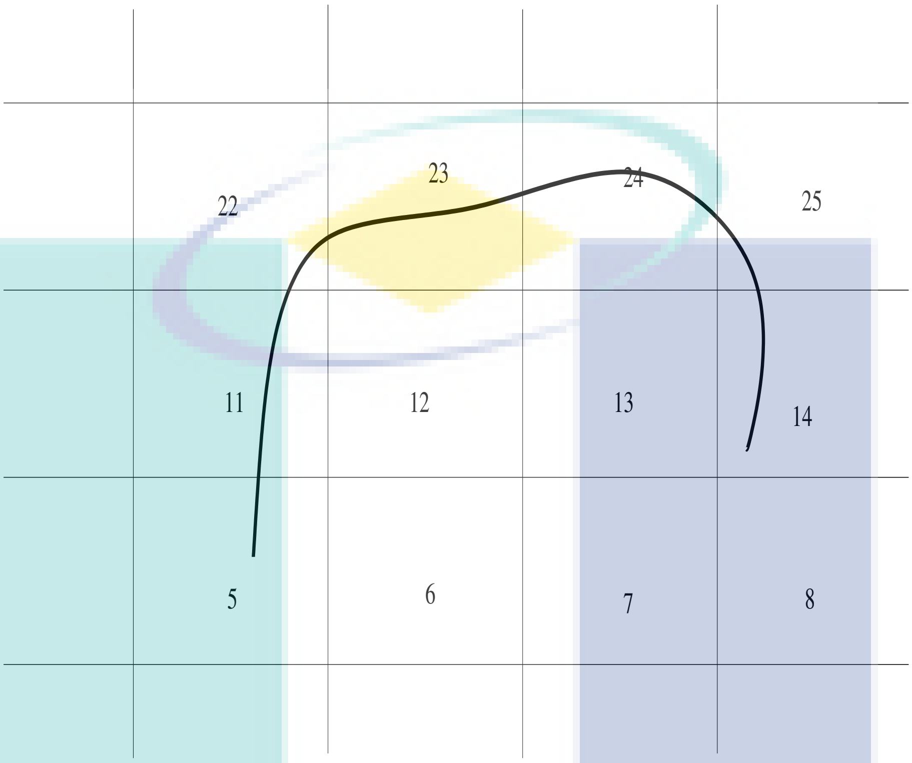

Figure 2.5. QDAS

The dynamic grid transformation component hides the process of drawing the design; thus, it tackles the *shoulder surfing* attack and hence, it is safer than the original *DAS* to this attack. Although, this scheme has higher entropy than its predecessor (Lashkari, Saleh, Towhidi, & Farmand, 2009), but it has lower memorability than the original scheme (Lin, Dunphy, Olivier, & Yan, 2007).

Background DAS (BDAS)

BDAS (Dunphy & Yan, 2007) introduces the idea of incorporating background images with the drawing grid of the original *DAS* scheme so that they can be used to provide a cued recall. Alike *QDAS*, a user has to select a grid as demonstrated in 2.6,

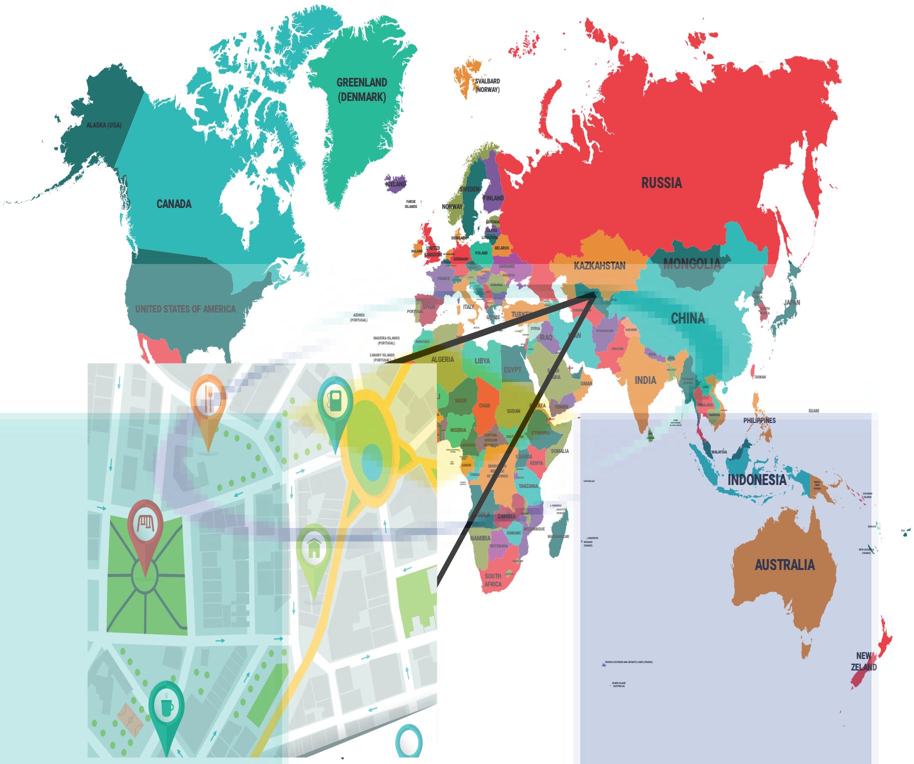

Figure 2.6. BDAS

which will be zoomed in afterwards, and s/he has to draw a design in it. It has been observed that the selection of the grid and the drawing is mostly influenced by the image that is placed at the background. Therefore, the background image must be chosen carefully so that each user who views such an image may take an interest in a different part of it—which would increase the variation of the secrets created by users, and thus, would make it more difficult to predict. To increase the usability of the scheme, a user is suggested to conceive a secret in his/her mind and reflect that through the drawing. Although, incorporating the background image with the original *DAS* increases the entropy of the scheme; however, it suffers from the *shoulder surfing* attack. Again, the quantity of “hot spots” plays an important role, since otherwise, many users would concentrate on specific territories while selecting grids (Wiedenbeck, Waters, Birget, Brodskiy, & Memon, 2005a).

Knock Code

This is a 2x2 *graphical* password which is one of the newest innovation in the area of smart phone authentication system. This scheme was introduced a few years back by a popular smart phone brand LG.

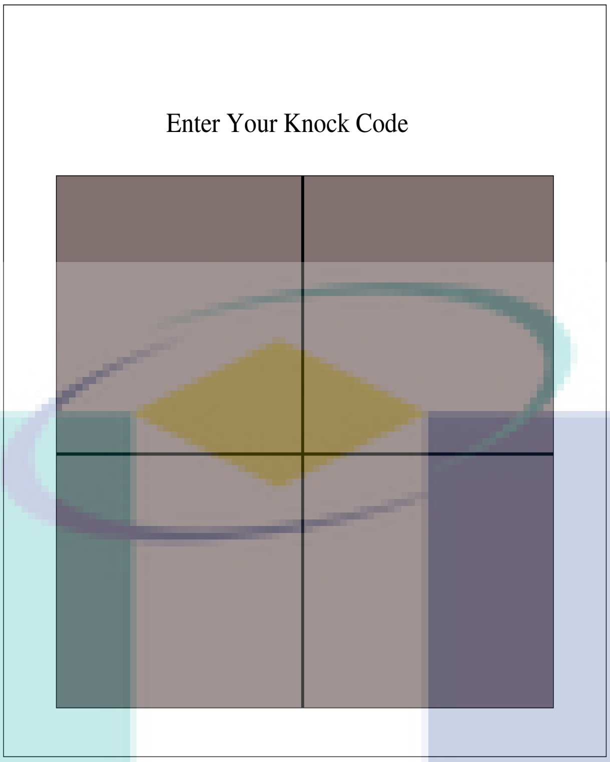

Figure 2.7. Knock Code

One of the main attraction of the system is that a user can give password at any place of the screen. A user needs to tap on the 2x2 grid several times—minimum 6 times— to get authenticated. User can assume this 2x2 grid anywhere on the screen.

Evaluation

In *Drawmetric* Schemes Each stroke contains data, for example in *DAS* each stroke consists of pen up, pen down, and the grids which the strokes cross. For schemes without any grids, each stroke includes the sequence of qualitative direction changes. So the formula of the theoretical password space for *Drawmetric* schemes can be analysed by following steps (Gao et al., 2013) Assume X_t denotes password with t strokes (one password can include m strokes at most). So the theoretical password space S can be deduced by:

$$M_R^S(x) : \tilde{G_{\alpha_x}} : \alpha_x : \sum_{i=1}^{i_x} PiS = \sum_{t=1}^{m} X_t \tag{2.2}$$

s_k is defined as the number of strokes with length k (stroke length can reach z at most), so the total number of stokes S_{total} can defined as:

$$M_R^S(x) : \tilde{G_{\alpha_x}} : \alpha_x : \sum_{i=1}^{i_x} PiS_{total} = \sum_{k=1}^{z} S_k \tag{2.3}$$

For a password with t strokes, all possible password space can be repeated to take the t strokes arrangement. Namely: $X_t = S_{total}$, So,

$$M_R^S(x) : \tilde{G_{\alpha_x}} : \alpha_x : \sum_{i=1}^{i_x} PiSp = \sum_{t=1}^{m} (\sum_{k=1}^{z} S_k)^t \tag{2.4}$$

Examples are presented to explain the universal formula. In gridded schemes (like *DAS*), S_k is defined as pen up, pen down, and the grids where the stroke crosses. Namely:

$$M_R^S(x) : \tilde{G_{\alpha_x}} : \alpha_x : \sum_{i=1}^{i_x} PiS_k = \sum_{(p,q)\in[1...X][1...X]} n(p,q,k,x) \tag{2.5}$$

n(p,q,k,x) is the number of strokes with length k and end at the cell (p,q). In a grid of XxX, it can be conclude:

$$\begin{aligned} M_R^S(x) : \tilde{G_{\alpha_x}} : \alpha_x : \sum_{i=1}^{i_x} Pin(p,q,k,X) = n(p1,q,k1,X) + n(p,q1,k1,X) \\ +n(p,q+1,k1,X) + n(p+1,q,k1,X) \\ +n(p+1,q-1,k1,X) + n(p-1,q-1,k1,X) + \\ n(p-1,q+1,k1,X) + n(p+1,q+1,k1,X) \end{aligned} \tag{2.6}$$

s_k denotes the sequence of qualitative direction changes. There are eight different possible directions shown in figure. While , k=1 :
$S_k = n(p,q,1,X) = 1$;
so , if k=2 and only 8 possible direction a password can use, then
$S_k = n(p,q,2,x) = 8$; so , if k=3 , then recursively the value of sk will be
$S_k = n(p,q,3,x) = 8x8 = 64$
same way for k=4,
S_k = n(p,q,4,x) = 64 x8 = 512
So , for stroke length k=4 , and number of stroke i=5, the password space will be :
$Sp = (512)^5 = 35184372088832$

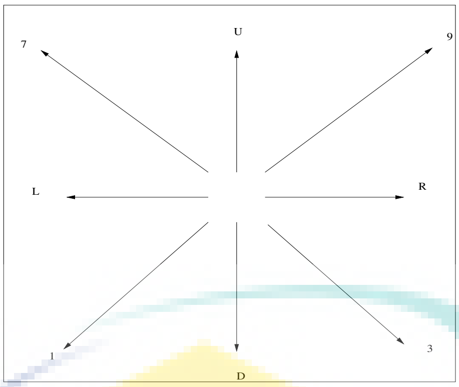

Figure 2.8. Possible direction of Drawmetric passwords

Table 2.1. Password space of Drawmetric scheme according to stroke length and Number of strokes

Drawmetric schemes		
Stroke Number (i)	**Stroke length** (k)	**Password Space**
5	2	32768
	4	35184372088832
	6	$1.15292150460685x10^{18}$
	8	$4.05648192073033x10^{31}$
	10	$4.35561429658801x10^{40}$
10	2	1073741824
	4	$1.23794x10^{27}$
	6	$1.32923x10^{36}$
	8	$1.6455x10^{63}$
	10	$1.89714x10^{81}$
15	2	$3.51844x10^{13}$
	4	$1.5325x10^{40}$
	6	$1.5325x10^{54}$
	8	$6.67496x10^{94}$
	10	$8.2632x10^{121}$

Table 2.1 represents a list of password space according to number of strokes and stroke length.

2.4.1.2 Locimetric Schemes

Locimetric schemes (Gao et al., 2013)—*a.k.a click-based graphical password* schemes—are based on the loci method, and hence the name (Perkins, 1979). In this class of scheme, several click points are selected from a given image or from a specified zone of a given image. A credential is considered matched when click points and their order of clicking is correct. Although there exist a considerable number of such schemes, some prominent schemes are described below.

Blonder

In *Blonder*—the first *graphical* password scheme that is proposed in 1996—a user is required to click on preselected areas (or on tag regions) of the pre-decided *graphica* image in a chronological ordered sequence, as a means of entering his/her credential (Blonder, 1996).

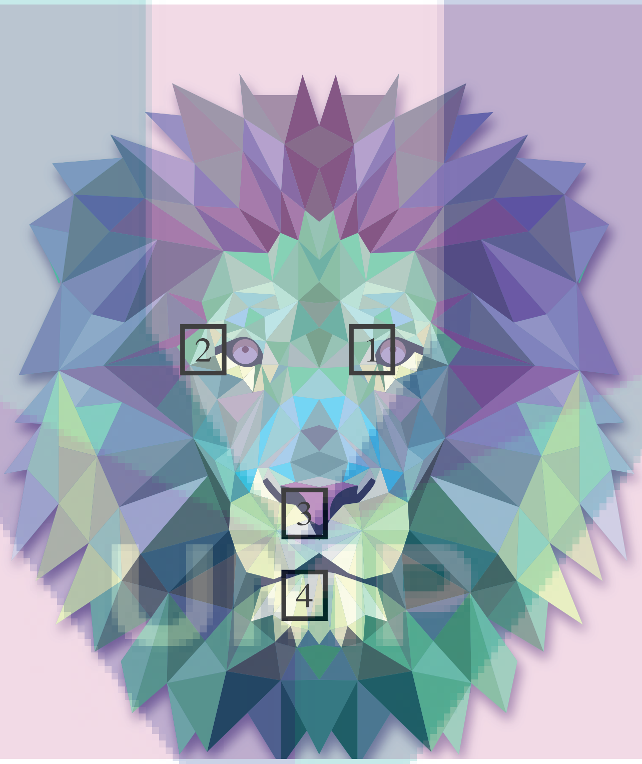

Figure 2.9. Blonder

It has several notable advantages over alphanumeric passwords, such as *i*) images are easier to recall, specifically images with personal meaning (Gao et al., 2013), i.e., memorability of this scheme is higher, *ii*) in terms of password space, this scheme offers a large password space over alphanumeric schemes; e.g., in an image of 3 *inch* × 5 *inch* with one-quarter inch square (6 *mm* × 6 *mm*) click points—it offers 13.6 million possible combinations for a selection of just 3 click points in the correct chronological order. In comparison to that a three-digit

PIN offers only 1,000 possible combinations and a three-letter credential offers only 17,000 possible combinations (Blonder, 1996). However, this scheme suffers from several limitations. For instance, in an image, number of click points are readily identifiable and they are limited in number—perhaps a few dozens in an image (Lashkari, Saleh, et al., 2009). For adequate security, a selected image must contain adequate number of click points. Moreover, it is vulnerable to *shoulder surfing* attack with compare to *text-based* schemes.

Pass Map

One of the main problems with passwords is that very good passwords are hard to remember and the one which are easy to remember are too short of simple to be secured. From the studies of

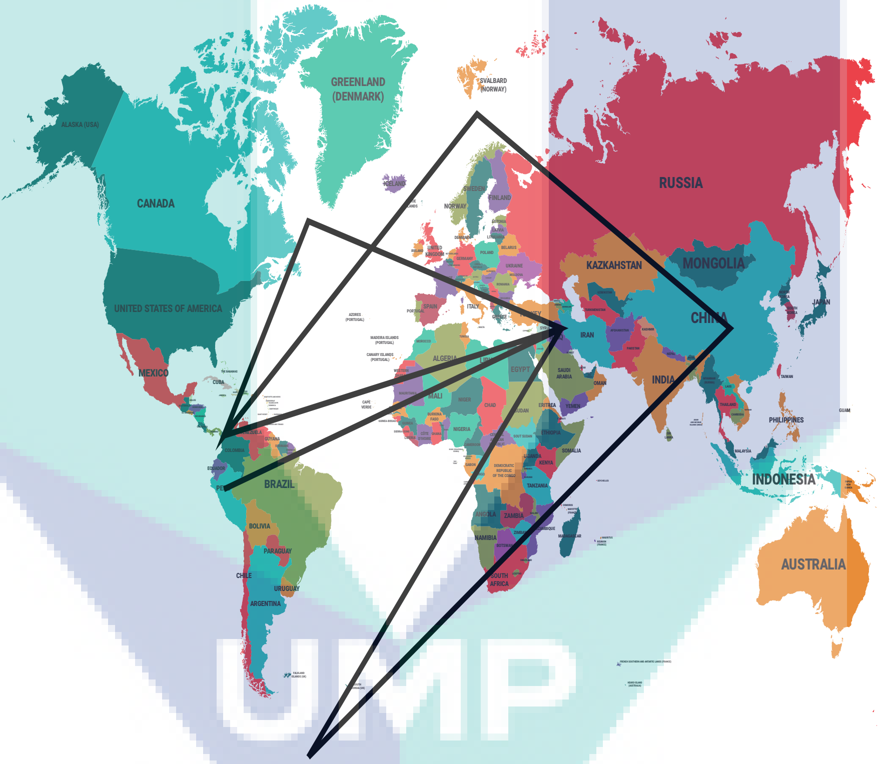

Figure 2.10. Pass Map

human memory, it is known that it is relatively easy to remember landmarks on a well-known journey. As an alternative example, a map of the Europe can be used and a user who has never been to Europe before should have no problem memorizing that he wants to one day see the Eiffel Tour in Paris, the Big Ben in London and the Kremlin in Moscow and his PassMap might be to visit all of them one at a time flying in from his hometown (Yampolskiy, 2007). Additionally the *Pass Map* technology is not very susceptible to *shoulder surfing* attack as it can be clearly seen from Noticing a single new edge in a large graph or even an absence of some edge in the map is not a trivial task, for someone just passing by. But with respect to *brute force* attacks while at the same time considering how good those mechanisms are in terms of how memorable they are (Lashkari, Saleh, et al., 2009).

Passlogix

Passlogix Inc. is a *New York* based business security organization, who proposes an authentication scheme, called *Passlogix v-Go*. In this scheme, a user has to repeat a sequence of actions following a chronological situation to form a credential. To increase the memorability of the user, s/he can employ any preferable background image, such as kitchen, washroom, room, or others as depicted in Figure 2.11.

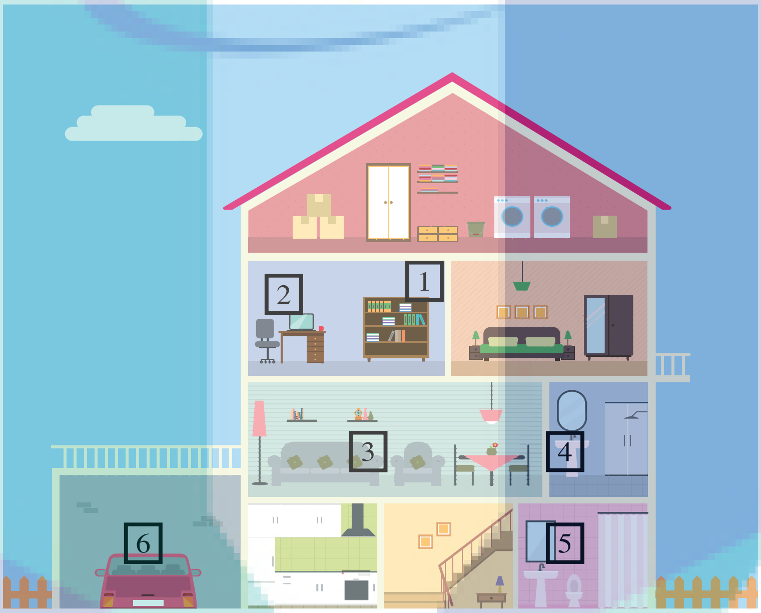

Figure 2.11. Passlogix

A credential can be registered by clicking and/or dragging on a progression of things inside that picture. For instance, a user can think of preparing a meal as a theme, where s/he can prepare a meal by selecting cooking ingredients, by taking a burger (fast food) from the refrigerator and putting it into the microwave oven, by selecting some fruits and washing them into a washbasin and then, putting them in a clean bowl (Abdullah, Abdullah, Ithnin, & Mammi, 2008). This scheme is vulnerable to several attacks and threats. For instance, due to the limited size of the password space, it is easily breachable to the *shoulder surfing* attack. Again, since the credential depends on the progression of things, it is somewhat guessable or predictable (Lashkari, Saleh, et al., 2009). Elaborately, lets assume that a user has registered a password such that some vegetables are dragged from their containers to a bowl. Now, there are limited places in the bowl and hence, can contain limited number of vegetables.

Evaluation

Locimetric schemes ask users to select several regions as a password in a given picture. Some schemes use predefined selected regions. Assume A available regions in a scheme. Users select at most r regions as their password. The universal theoretical password space formula for this type of schemes is:

$$M_R^S(x) : \tilde{G_{\alpha_x}} : \alpha_x : \sum_{i=1}^{i_x} PiT = \sum_{i=1}^{r} A^i \qquad 2.7$$

Other schemes ask users choose dots as passwords in a given picture. Because users only click on a pixel, the system can set the pixel as center, and select a certain threshold value of P_0 as the password region. Users must remember the sequence in the password region. P denotes the area of the picture, and the theoretical password space is:

$$M_R^S(x) : \tilde{G_{\alpha_x}} : \alpha_x : \sum_{i=1}^{i_x} PiT = \sum_{i=1}^{r} (\frac{P}{P_0})^i \qquad 2.8$$

For this example, a $460x340$ picture is used, with a square size of $30x30$. The user can choose 5 to 10 points as a password. Using the universal theoretical password space formula and the theoretical password space can be found :

$$T = \sum_{5}^{10} (\frac{460x340}{30x30})^i \approx 2.512x10^{22}$$

Table 2.2. Password space of locimetric scheme according to Square Size and Picture Resolution

Locimetric Schemes		
Picture Resolution (P)	**Square Size (P_0)**	**Password Space**
$640x480$	$30x30$	$2.14677742252744x10^{25}$
	$50x50$	$7.84895839231035x10^{20}$
	$80x80$	$6.4925062108545x10^{16}$
$800x600$	$30x30$	$1.86203259627767x10^{27}$
	$50x50$	$1.20892581961463x10^{24}$
	$80x80$	$5.63135147094727x10^{18}$
$1024x768$	$30x30$	$2.59529465505917x10^{29}$
	$50x50$	$9.4888084575449x10^{24}$
	$80x80$	$7.84895839231035x10^{20}$
$2560x1440$	$30x30$	$1.32922799578492x10^{29}$
	$50x50$	$4.85986815555701x10^{31}$
	$80x80$	$4.0199887178406x10^{27}$

A list of password space of emphlocimetric schemes are given in the Table 2.2

2.4.1.3 Cognometrics schemes

In these schemes, a.k.a., *Cognometrics* schemes, a user creates a credential by selecting several images from a large portfolio of images. Afterwards, during the authentication session, the user has to repeat the selection from decoy images (Gao et al., 2013). Here, a system relies on recognition rather than recall, which makes an authentication more easier and trustable (Dhamija & Perrig, 2000).

Pass Face

Pass face is a *graphical* secret word conspire, for which the helplessness and convenience has been generally under investigated (Dunphy, Nicholson, & Olivier, 2008). They are *graphical* passwords, that is usefull as a remarkable check innovation for secure logon (Brostoff & Sasse, 2000). The creator of Passfaces has patented a method of using faces to facilitate PIN recall by creating an intuitive mapping between faces and PIN digits (Davies, 1999). The enrolment methodology permits clients to first choose whether their Passface set is male or female. They then select 4 confronts, and are coordinated to consider the qualities of their determinations, and why they chose them. The clients are then twice taken through the Passfaces login method, with their Passfaces demonstrated to them. They finish enrolment by accurately recognizing their 4 Passfaces twice in a push with no inciting, then (in this field trial just) entering an enrolment secret word (Brostoff & Sasse, 2000). To sign in, clients select their Passfaces from a grid of faces showed on the screen (Brostoff & Sasse, 2000). Passfaces were appeared to be memorable in a review including 77 staff and understudies of Goldsmiths College (Valentine, 1998) All members experienced the Passfaces enrolment method, and 3 conditions were tried. The main condition had 29 members signing in each working day for 2 weeks. Members accurately reviewed their Passfaces in 99.98% of logins. The second condition had 29 members sign in roughly 7 days after enrolment. On their first endeavor, 83% signed in effectively. Everybody in this condition signed in by his or her third endeavor. The third condition had 19 members login just once roughly 30 days after enrolment, with 84% of members recollecting their Passfaces at the to start with endeavor, and the rest of their Passfaces by the third endeavor (Valentine, 1998). Brostoff and Sasse (Brostoff & Sasse, 2000) led an assessment of the system in a field study that found that members utilizing Passfaces experienced 33% of the login mistakes of alphanumeric secret key clients, regardless of getting to the system less every now and again.

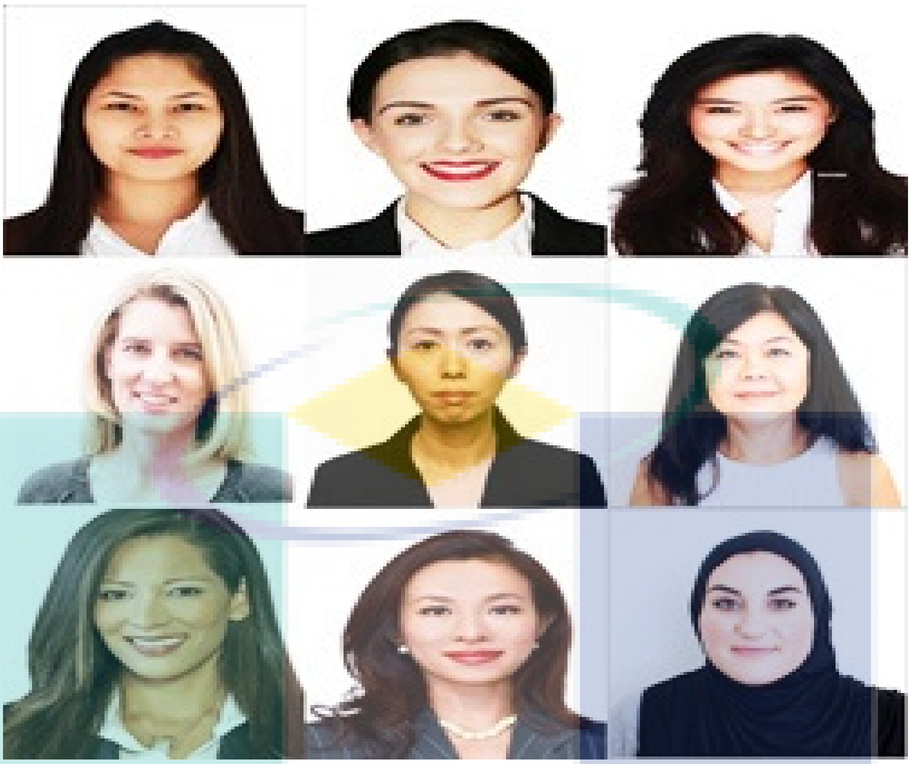

Figure 2.12. Pass Face

One claimed advantage of the *Pass Face* scheme over conventional alphanumeric passwords is that Passfaces cant be written down or copied and cant be given to another person (Authentication, 2004). A number of subtle configurations have been adopted to mitigate against the isk of easy description, such as that the grids of faces in Passfaces are grouped by sex and are selected to be equally distinctive so that Passfaces cannot be described by gender or obvious characteristics. None of the faces stand out from the others (Authentication, 2004), Among different issues, members felt that because of the obvious trouble of recording their passfaces they had no system in connection to overlooking (i.e. they had a practical consciousness of the trouble of composing down their passfaces). Valentine found that users memory for passfaces was altogether superior to for traditional passwords (Dunphy et al., 2008). Passwords had a login failure rate of 15.1%, while Passfaces for the same participants produced a login failure rate of 4.9% (Brostoff & Sasse, 2000). But *Pass face* set aside a long time to execute (Brostoff & Sasse, 2000) *Other unpublished assessments led by Valentine (Valentine, 1999) (Valentine, 1998) found that user had low desires that they would recall passfaces over a long timeframe. Among different issues, members felt that because of the clear trouble of recording their passfaces they had no procedure in connection to overlooking (i.e. they had a rational attention to the trouble of composing down their passfaces). Valentine found that clients' memory for passfaces was fundamentally superior to for ordinary passwords.

Picture Password

Picture Password is a visual login system that matches the abilities and confinements of most handheld gadgets and gives a straightforward and instinctive route for users to authenticate. Other than user authentication, *Picture Password* may likewise be utilized as a part of other security applications where ordinary passwords have been utilized generally. While the arrangement is especially appropriate for handheld gadgets, *Picture Password* can likewise be utilized as a part of an extensive variety of registering stages (Jansen, 2004).

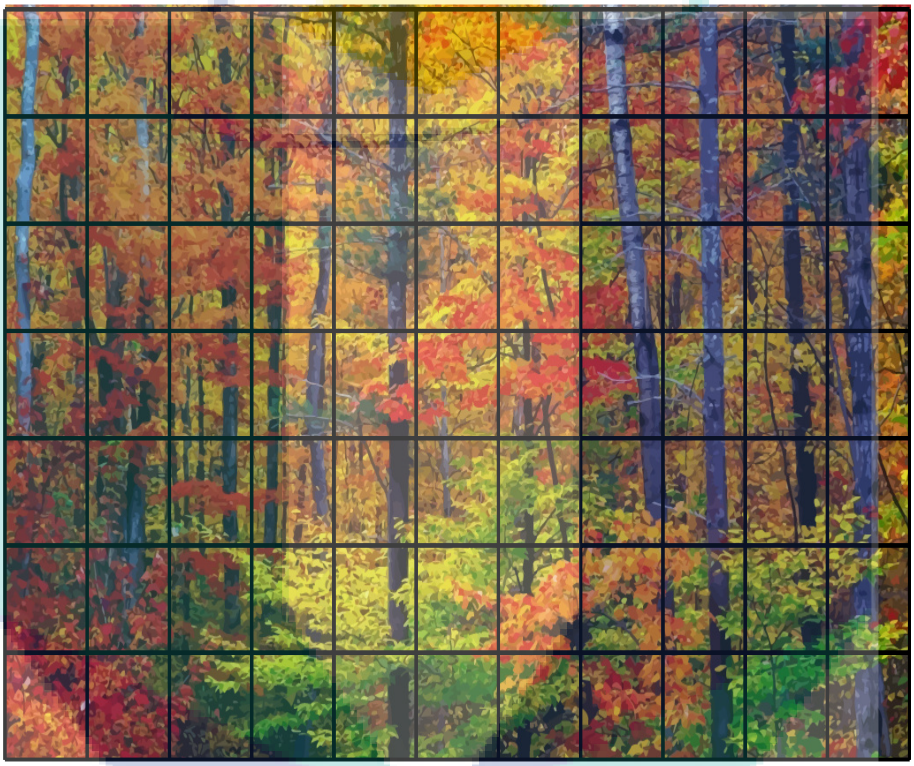

Figure 2.13. Picture password

Similarly as with *textual* password authentication systems, *Picture Password* employments components of a letter set to frame a password entry of a given length. In any case, rather than the user remembering a string of arbitrary like alphanumeric characters, the succession of pictures that frame a password must be recalled and chosen. In addition, a picture arrangement that makes them mean or is of intrigue to the individual user (e.g., pictures of game group logos all together of inclination) can be utilized. If forgotten, the grouping might be reproduced from the innate visual signs (Jansen, 2004). The presentation of visual pictures to the user for choice depends on tiling an region of the *graphical* interface window with thumbnail pictures. Different ways exist to tile a range, the least difficult being squares of indistinguishable size gathered into a two-dimensional matrix. The surface of every tile shows a bit-mapped representation of some thumbnail picture provided in a predefined digital format. The objective is to strike a harmony between giving clear recognizable and effectively selectable pictures inside the show zone and having an adequate number to empower the development of solid passwords. *Picture Password* utilizes a format of 30 indistinguishably estimated squares for its thumbnail pictures, assembled into a 5x6 matrix At the point when a picture sequence is at first selected, users can choose among a different accessible predefined themes (Jansen, 2004). A choice exists to rearrange pictures between confirmation attempts, where suitable for the topic, to make include observing by an observer troublesome (Jansen, 2004). Each thumbnail picture is distinct and independently conspicuous, a few of them may be utilized by and large to shape a composite mosaic picture. users may characterize new topics utilizing a topic developer device and their own particular pictures.

Story Scheme

In 2004, the story plot proposed by classifying the accessible picture to nine classes which are creatures, autos, ladies, nourishment, kids, men, articles, nature and game. As indicated by Fig 2.14, the user need to choose their passwords from the blended pictures of nine classifications with a specific end goal to make a story effectively to remember. There were a few users who utilized this technique without characterizing a story for themselves (Davis, Monrose, & Reiter, 2004). In the Story conspire, a user's password is arrangement of k extraordinary pictures chose from one arrangement of n pictures, appeared above, to delineate a "story". Here, n = 9, and pictures are set arbitrarily in a 3*x*3 grid (Towhidi & Masrom, 2009). This research demonstrated that the story plan was harder to keep in mind in contrast with Passface validation (Davis et al., 2004). In this thoery, biasness effect a lot on user while giving a password (Davis et al., 2004).

Evaluation

Cognometric schemes differ from other *graphical* password schemes in that they display pictures for users to recognize, and for easy to recognize, the pictures must not be too small. At present, Cognometric schemes usually include an image library with size S. Users password pictures include m pictures at most. There are two kinds of circumstances in the password picture: orderly and disorderly. The orderly theoretical password space is:

$$M_R^S(x) : \tilde{G_{\alpha_x}} : \alpha_x : \sum_{i=1}^{i_x} PiT_{order} = \sum_{k=1}^{m} P_s^k = \sum_{k=1}^{m} (\frac{N!}{(N-k)!}) \tag{2.9}$$

The disorderly theoretical password space is:

$$M_R^S(x) : \tilde{G_{\alpha_x}} : \alpha_x : \sum_{i=1}^{i_x} PiT_{disorder} = \sum_{k=1}^{m} C_s^k = \sum_{k=1}^{m} (\frac{N!}{(N-k)!k!}) \tag{2.10}$$

Using Story as an example, the picture library has 150 images is assumed, and the users password images are between 5 and 10. According to the formula, the theoretical password space can be computed :

Figure 2.14. Story Sceheme

$$T_{disorder} = \sum_{5}^{10} P_{150}^{k} \approx 4.27x10^{21}$$

From given examples and investigation undertaken in this thesis, it can infered that the universal formulas are suitable for concrete schemes and give a general comprehension of password space.

Table 2.3 represent a list of password space according to total pictures and maximum selected passwords among them.

2.4.1.4 Sui Generis

These schemes, a.k.a., *Sui Generis*, are the unique authentication schemes, which are either the combinations of different *graphical* authentication schemes or any uncommon scheme which are not similar to any of the above schemes.

V.A.P Code

VAP is a unique authentication system which is the combination of *Pattern Lock*(2.4.1.1) and VC(Vibration Code) with some new ingredients. A *VAP* code is a code which comprises of multiple VCs acquired from multiple grid cells and that yields a PL when VCs are acquired. Consequently, when a user endeavors to unlock a screen, along with the VCs, the PL is also necessary to be matched.This system consist of screen(any size) with 4 grids of exact

Table 2.3. Password space of Cognometrics schemes according to Total pictures and maximum selected pictures

Cognometrics Schemes		
Total Pictures (P)	**Max selected (m)**	**Password Space**
100 (order)	5	9034502400
	10	6.28156509555295$x10^{19}$
	20	1.30399501820471$x10^{39}$
150 (order)	5	70992003600.0001
	10	4.24407863738912$x10^{21}$
	20	8.83487185691629$x10^{42}$
100 (disorder)	5	591600030.000001
	10	1.16955429822231$x10^{15}$
	20	3.63141294931877$x10^{24}$
150 (disorder)	5	591600030.000001
	10	1.16955429822231$x10^{15}$
	20	3.63141294931877$x10^{24}$

same size. Prior using the proposed *graphical* password scheme, a user must register himself/herself to the system by providing a preferred *VAP* code. A user has the freedom to start sensing vibration from any grid cell among the four cells. The vibration starts when a user establishes his/her finger on a cell. after sensing a consecutive vibrations (which is between 1-10), the user moves to the next cell (anycell). When a user moves his/her finger beyond a certain threshold pixel without leaving the grid area or if user take off his/her finger from the screen, the system stops generating any vibration. All the acquired values are then stored in their respective multisets for future authentication. In the authentication phase user needs to do the same activity with the screen and grids like he did in registration phase.Vibration-And-Pattern *VAP* code, which offers protection against these three major attacks. It defends brute force attack by offering a larger password space, and ensures resilience against other two major attacks: shoulder surfing and smudge attacks. Although,this system gains resilience against three aforementioned major attacks, however, it may experience another unusual attack, called *timing* attack. (Azad et al., 2016)

2.5 Press Touch Technique

Touch screen of smart device was first introduced back in 1992 (*The Touching History of Touchscreen Tech*, n.d.) in IBM Simon. Later on in 2007 iPhone brought the most usefull and furnished version of touch screen (*History of the iPhone 2007-2017: the journey to iPhone*

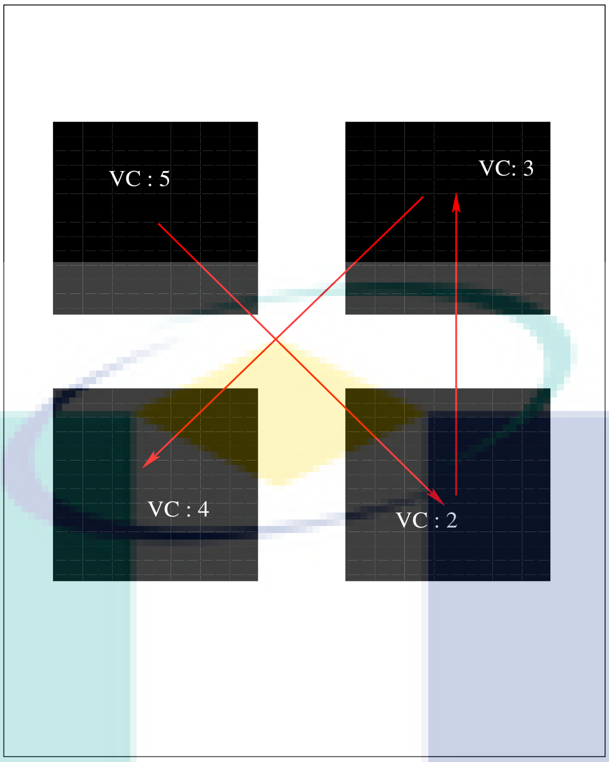

Figure 2.15. V.A.P CODE

X, n.d.). Since then the technology (on the consumer front) has not changed yet. Touch screens is capable to sense multiple touches (one, two, three fingers, etc) by which user can swipe, pinch, and pan around the screen. The press touch display was first found in the iPhone 6s which is the next evolution of the multi touch display (*Take Advantage of 3D Touch*, n.d.). It can also sense multiple points of input, it can sense the intensity of the pressure the user is applying to the screen. Lighter press gets one action also harder press gets another action. It is the act of pressing harder which produces pressure and on a minuscule level allows finger to press into the displayhence interacting with it in three dimensions.Press touch technique is a tiny motorized engine which is similar to the motor that creates vibrations in phone already. When the Press Touch sensitive display senses pressure is being applied to the display, it provides a haptic feedback via tiny pulses that are generated in the Taptic engine. Later on press touch technique has started get integrating in different other Android OS based smart phone, such as, Huawei P9 Plus.

2.6 Critical Analysis

This section compares the most relevant authentication schemes, e.g., PIN (Personal Identification Number), AN (Alphanumeric Number), APL (Android Pattern Lock), VAPC (*VAP* Code) and KC (*Knock* Code) based on some key parameters, such as, *shoulder surfing*, *brute force*, and *smudge* attack resilience, also, screen size independency, and authentication process time. These schemes are given a mark of H (high), M (medium) and L (low) according to their performance in terms of those parameters. Specific reasons for their making are also argued briefly.

Table 2.4. Comparison of prominent related schemes with each other

Attack/Function	**PIN**	**AN**	**APL**	**VAPC**	**KC**
Shoulder surfing	H	H	H	L	M
Brute force	H	M	M	L	L
Smudge	M	M	H	L	L
Screen Size Independence	N	N	N	N	Y
Short Authentication Time	Y	Y	Y	N	Y

As shown in the Table 2.4, PIN and AN are declared highly risky for *shoulder surfing* attack. Because, while a user provides PIN or an AN on a keyboard, there are high possibilities of getting the password by sneaking into it or setting a camera nearby (Zhao & Li, 2007) (Roth, Richter, & Freidinger, 2004) (Bianchi, Oakley, Kostakos, & Kwon, 2011). Although, the smudge attack is not extremely risky for these two schemes, but still there is a minor risk. There is a slight possibility of identifying the password by tracking the smudges created on a screen (Aviv et al., 2010) (Von Zezschwitz, De Luca, Brunkow, & Hussmann, 2015). PIN is immensely vulnerable to *brute force* attack (Bond & Zieliński, 2003) (Viehböck, 2011) due to their lower password space—maximum combination for a PIN with 6 digits is only $10^6 = 1000000$. AN is also vulnerable in terms of this attack, but not as much as PIN. Because, its password space is a bit higher than that of the PIN—maximum combination for an AN with 6 digits/characters is $256^6 = 2.8147498 \times 10^{14}$ as the total number of ASCII characters are 256 (Pareek, Patidar, & Sud, 2005). In terms of authentication processing time, both PIN and AN can complete authentication within a very short period of time (De Luca, Langheinrich, & Hussmann, 2010). However they are not screen size independent. Due to this, they cannot be functional in small screen size devices, e.g., smart watch, smart band, and so on. Unlike, PIN and AN, both APL and VAPC are *graphical* passwords. Although APL is a pure *graphical* password, VAPC is a combination of *graphical* and sense based password, which is determine in section 2.4.1.4. APL is immensely defenseless against *shoulder surfing* attack (Kwon & Na, 2014) (Song, Cho, Oh, Kim, & Huh, 2015). While a user is drawing a pattern on the screen. It could be determine by someone by observing from a certain distance. On the other hand, VAPC has a great defense against the *shoulder surfing* attack (Azad et al., 2016). Even if the intruder is somehow successful to acquire the sequence of pattern given, still there is a very low possibility that the number of vibrations given in each grid could be attained. In case of the *smudge* attack, VAPC has a good resistance against this attack, where as the resilience of APL is extremely low in this case (Kwon & Na, 2014) (Andriotis, Tryfonas, Oikonomou, & Yildiz, 2013) (Aviv et al., 2010). Because, under a certain light projection a user's pattern is quiet easy to identify from the smudges which are left on the screen (Aviv et al., 2010). When it comes to the case of *brute force* attack, guessing a user's pattern is bit difficult, but still not beyond concern (Kim, 2012) (Andriotis et al., 2013). On the other hand, VAPC got a pretty good defense against the *brute force* attack compare to APL.

Table 2.5. The password Space, P, for the VAPC when $\mu = 10$ vs APL.

L	**VAPC**		**APL**
	P_v	P	P
1	10	40	9
2	100	1200	56
3	1000	36000	320
4	10000	1080000	1624
5	100000	32400000	7152
6	1000000	1072000000	26016
7	10000000	32160000000	72912
8	100000000	964800000000	140704
9	1000000000	28944000000000	140704

In Table 2.5, an illustration of password space for various L (the number of grids/dots visited) values is given for $\mu = 10$ (μ is the Highest number of consecutive vibrations a device generates for authentication process (Azad et al., 2016)). It shows that higher L values provide a greater security. When compared with the APL, VAPC offers a considerably higher password space. The reason of APL's limited password space is due to several restrictions (Andriotis et al., 2014), such as i) each pattern must connect at least four dots, ii) the dots in the pattern must all be distinct, and iii) if the line segment connecting any two consecutive dots in the pattern passes through any other dots, the other dots must have previously been in the pattern. Considering these restrictions, the maximum number of distinct patterns possible is 389,112 (Aviv et al., 2010). In contrast, VAPC outperforms APL even when $L \geq 4$. Again VAPC offers a large password space, it is difficult to break using *brute force* attack. In case of authentication processing time, APL can complete the authentication process very quickly, because of its simple and easy authentication steps (Andriotis et al., 2014). On the other hand, VAPC spends a considerably longer duration for authentication. For instance, for a total *VC* of β_t (where $\beta_t \in \mathbb{Z}^+$), the authentication duration lies between $(\beta_t \times \tau_{min} + |Q| \times \tau_g)$ to $(\beta_t \times \tau_{max} + |Q| \times \tau_g)$, where τ_g is the average interval to move from one grid to another grid. If $\tau_{min} = 300ms$, $\tau_{max} = 900ms$, $|Q| = 4$, $\beta_t = sum(S) = 10$, and $\tau_g = 250ms$, then the duration of authentication lies between 4 seconds to 10 seconds (Azad et al., 2016). In compare to other existing schemes, it is a considerably large duration. Both the schemes are not screen size independent, because they need a minimum standard screen size for their grid cells/dots.

Due to this, they are also totally inapplicable for most of the tiny screen size smart device, e.g., smart watch, smart band, and so on.

Knock Code is a tapping based *graphical* authentication scheme which come with all new LG smart devices (*LG V20 KNOCK ON AND KNOCK CODE*, 2017). It offers a moderate security protection against the *shoulder surfing* attack. Attackers might be able to identify the number of taps given by sneaking into it. However as the user can use any place of the screen, it will be a bit tough for the attackers to discover the entire password correctly. *Knock code* has a very shallow risk in case of *smudge* attack. Its taps are very difficult to identify by observing smudges, because users can tap at the same place of the screen. But it is quiet defenseless against the *brute force* attack, as of the 4 grid, which results in a limited password space. Only one tap is allowed to provide each time when the user is visiting any grid. It works perfectly on any screen size when a single grid is considered, but offers a very limited password space. It is also very quick in finishing authentication process.

From the above discussions, it is evident that most of *graphical* password schemes currently available are not screen size independent and vulnerable to various major attacks. Therefore, it still remains one open research issue to investigate. The screen size independent *graphical* password scheme which is proposed in this paper is resilient against three major attacks: shoulder surfing attack, smudge attack, and brute force attack. The detailed proposed scheme are in subsequent chapter.

2.7 Summary

This chapter discusses the background knowledge that is essential to understand this thesis. Initially, a taxonomy is proposed where all the existing schemes are divided into two classes, namely *Elementary* authentication scheme and *Backup* authentication scheme, then again *Elementary Authentication Scheme* got divided into 2 subclasses, namely *memorization* based authentication and *non-memorization* based authentication. Afterwards, they are further divided into several subclasses. Since all the subclasses are not in-line, therefore, further discussions are limited to those classes that are similar to the proposed scheme. Again, since every class has numerous of schemes, so, only prominent schemes are described, scrutinized, and analysed with their advantages and limitations—which inspires to propose a new scheme. Also the ossible attacks on these schemes are analysed and summarized them in various tables. Furthermore, evaluation metrics for various schemes are also mentioned with various comparison tables. At the end the most related schemes are deeply investigated and their efficiency and drawbacks are highlighted.

CHAPTER 3

METHODOLOGY

3.1 Preamble

The research methodology part contains TWO (2) essential procedures: i) proposed scheme; and ii) evaluation setup (see Figure 3.1). Under the first procedure, three variants of the newly proposed scheme are discussed with their technical details, namely mono-PTC, multi-PTC, and multi-PTC with Grid. In addition, the registration and authentication process are explained elaborately. Again, the process of mono-PTC are devided into THREE (3) parts: i) data Acquisition; ii) data cleaning; and iii) Press Touch Finding. Note that the other two variants are the enhancement of mono-PTC to increase the level of security. In the second procedure, parameters for measuring the performance of the proposed scheme are briefly described. Afterwards, the in-lab experiment and the comprehensive survey that have been conducted to evaluate the effectiveness of the proposed scheme are elaborated. The lab experiment has been performed to discover the resilience of the system against the *shoulder surfing* attack. On the other hand, the comprehensive survey has been conducted to determine the usability of the proposed scheme.

3.2 Proposed Scheme

In this thesis, a new authentication scheme is proposed, which exploits the existing *Press Touch (PT)* technique of various smart devices by transforming it to a new type of code, named *Press Touch Code (PTC)*. Generally, *PT* is utilized to produce haptic feedback and to elicit a different set of responses depending on the intensity of the pressure applied on the touchscreen. This technique is also known as *Force Touch* in Apple's MacBook, Apple Watch, ZTE's Axon 7 phone; *3D Touch* in iPhone 6 and 7; and so on. In this thesis, the term—*Press Touch*—is adopted since Huawei (Huawei., n.d.) has given this name to their *Pressure Sensitive Technique (PST)* and the proposed scheme has been implemented and tested on one of the Huawei devices; more specifically, Huawei P9 Plus. This scheme is also directly applicable to other *PST* enabled *Android* devices. It also could be enabled to other similar devices of different operating systems with necessary modifications. Note that the pressure sensitivity technique is never been utilized as an authentication scheme; and hence, *PTC* is the first of its kind. However, it has a lot of potentials, which is exploit in this work. The *PTC* could

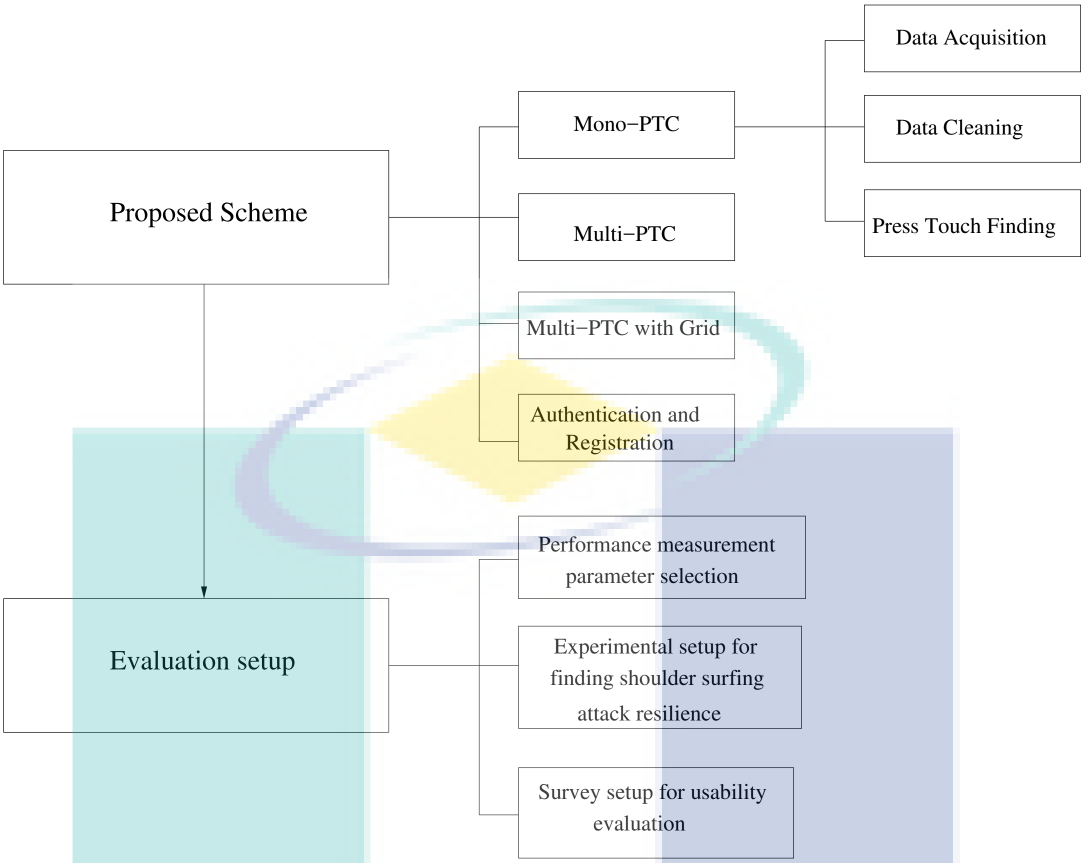
Proposed Scheme
Mono−PTC
Data Acquisition
Data Cleaning
Press Touch Finding
Multi−PTC
Multi−PTC with Grid
Authentication and Registration
Evaluation setup
Performance measurement parameter selection
Experimental setup for finding shoulder surfing attack resilience
Survey setup for usability evaluation

Figure 3.1. Methodology process flow

be utilized as a stand-alone authentication scheme or for higher security, it could be extended with multiple similar codes or again the latter also could be enhanced by incorporating grid cells in it. Let's distinguish them by calling mono-PTC, *multi-PTC*, and *multi-PTC with Grid*, respectively. Since the latter two variants are the extended version of the former variant; therefore, for grasping the idea of these variants, the detail knowledge about the former one is mandatory. Consequently the subsequent discussions are arranged accordingly.

3.2.1 Mono-PTC

When a user places a finger on a screen, the *Pressure Sensitive Screen (PSS)* can recognize the intensity of the touch. Let's denote this as ζ_{t_0}, which is the intensity of the press at time t_0. Afterwards, the intensity of the press is measured after every Δt time unit. This measured value ranges between 0 to 1, where 1 is for the most intense press and 0 is for no touch on the screen. For that reason, the press intensity value of a *PT* shows direction towards 1. In the proposed scheme, these values are utilized to generate a code, which would be considered as a password or signature of a particular user. In this thesis, password and signature terms are used interchangeably.

The entire process of placing a finger on the screen to proving *PT*s to generating *PTC*s could be divided into three phases, namely *i*) data acquisition, *ii*) data cleaning, and *iii*) press

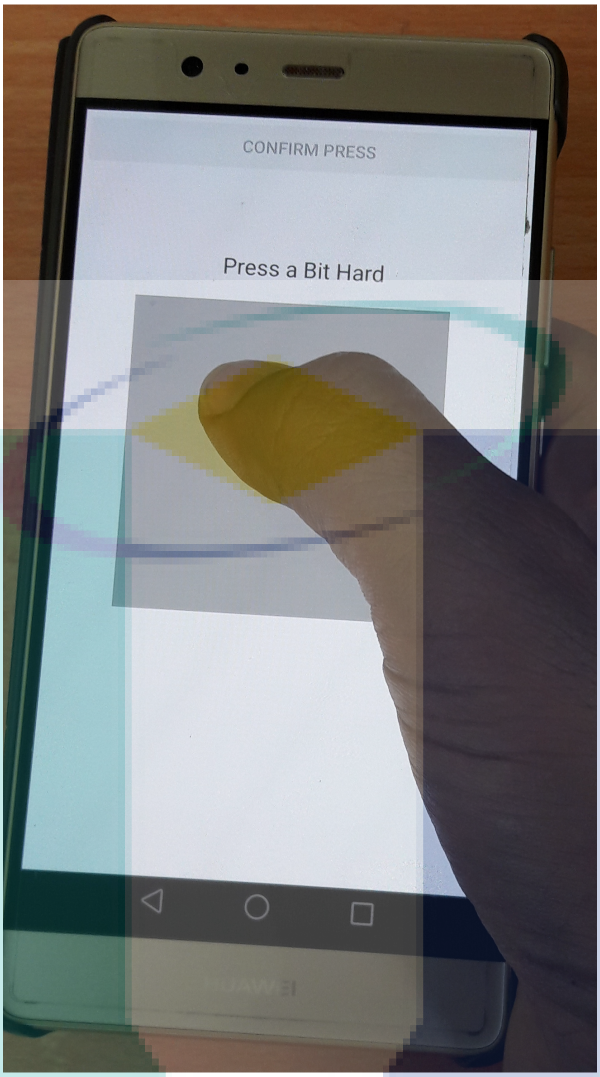

Figure 3.2. A user places a finger on the screen within the given square box, which starts the data acquisition process.

touch finding. All these phases are discussed below in details.

***Data Acquisition*:** The data acquisition phase starts when a user places a finger within the given box on the screen as shown in both Figure 3.2 and Figure 3.3. Although, data could be acquired from any place on the screen, but the box is given to expel any confusion that may arise in deciding where to press. Let's assume that ζ_{t_0} is the first press intensity value acquired at time t_0. Afterwards, the data acquisition process keeps acquiring press intensity values after every Δt time unit and stores them in a vector, ζ, where $\zeta = \{\zeta_{t_0}, \zeta_{t_1}, ..., \zeta_{t_n}\}$, $0 \leq \zeta_{t_i} \leq 1$, and $t_{i+1} - t_i = \Delta t$ where $i = 1, 2, 3, ..., n$. During this process, a user provides a desire *PTC* by pressing forcefully—which is a.k.a. *PT*—for that number of times. For instance, if a user has decided a *PTC* of k, where $k \in \mathbb{Z}^+$, then s/he must provide k *PT*s or in other words, press forcefully for k number of times. The whole procedure must be quick and sharp; otherwise, noise will be introduced due to finger movement as fingers seldom remain steady (Hudgens, Fatkin,

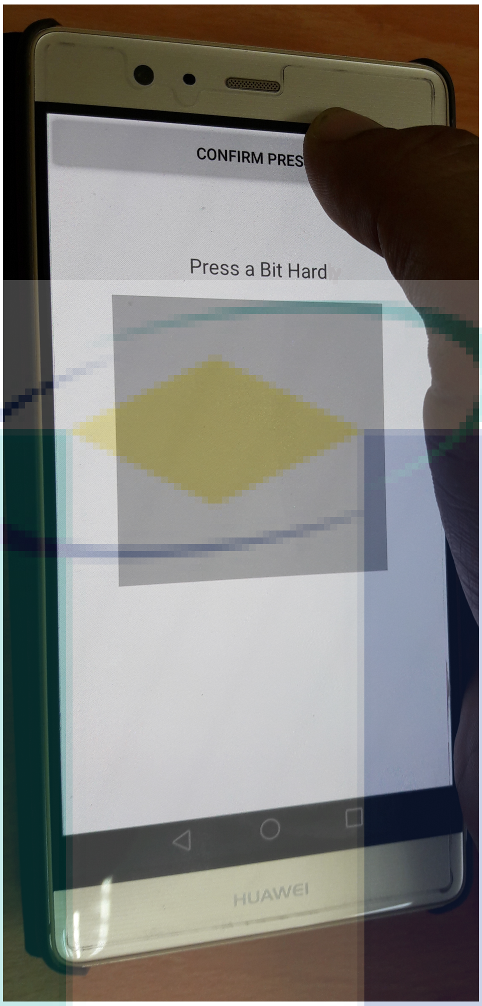

Figure 3.3. Data acquisition finishes when the user lifts the finger from the screen. The further processing will not start until the user press the confirmation button.

Billingsley, & Mazurczak, 1988). To end the data acquisition procedure, a user must lift the finger from the screen. Once all the data are acquired, they are cleaned and processed later to extract the *PTC*. The subsequent phases will not begin until the user presses the confirmation button as shown in Figure 3.3.

***Data Cleaning*:** In this phase, the acquired data are cleaned to remove unwanted noises from them. For extracting exact *PTC*, this phase is immensely important since any noise in the data can hamper the calculation. Moreover, a clean data simplify further processing.

In the proposed technique, *Moving Average Filtering Technique (MAFT)* (Smith et al., 1997) is employed for cleaning the acquired data. In *MAFT*, the data are smoothed by replacing each data point with the average of the neighboring data points defined within a span. For this, following equation (i.e., equation (3.1)) has been applied on ζ:

$$\zeta'_{t_i} = \frac{1}{2N+1}\left(\zeta_{(t_i+N)} + \zeta_{(t_i+N-1)} + \dots + \zeta_{(t_i-N)}\right) \qquad 3.1$$

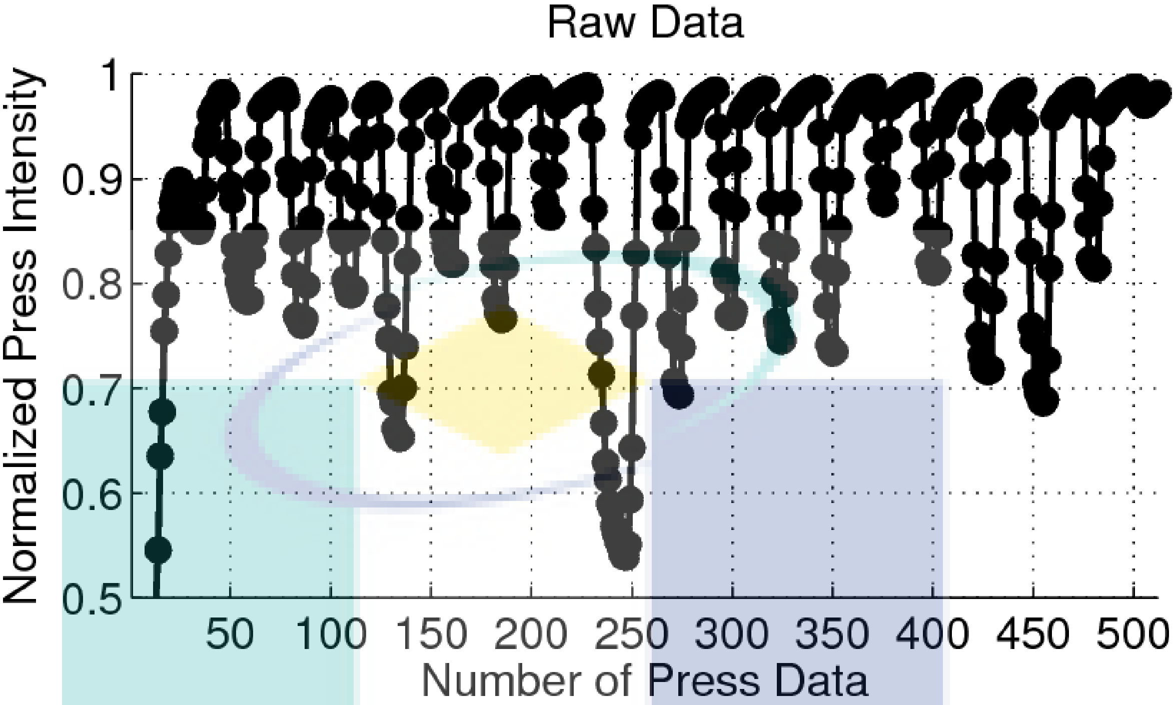

Figure 3.4. The acquired raw data

where ζ'_{t_i} is the press intensity value after smoothing process for the ith data point, N is the number of neighboring data points on either side of ζ_{t_i}, and $2N+1$ is the span. In Figure 3.4, an example of smoothing operation is shown for three N values, namely 1, 2, and 3; and thus, three span values, namely 3, 5, and 7, respectively. Although, $span =$ 5(see figure 3.6) and 7(see figure 3.7), clean the data more than $span = 3$(see figure 3.5); however, in some cases, they flatten the peak and impose complexity in finding the code. Therefore, in the proposed scheme, $span = 3$ is adopted, which smoothes the data considerably enough for finding the exact code by employing a simple algorithm. Afterwards, $\zeta_{t_i} \leftarrow \zeta'_{t_i}$, and ζ'_{t_i} is erased.

Press Touch Finding: As it could be observed from the Figure 3.4 is that when a user provides a *PT*—a peak is generated. Therefore, in the rest of the discussion, these two terms are utilized interchangeably. Any suitable *1-D Peak* finding algorithm (Cormen, Leiserson, Rivest, & Stein, 2001) could be utilized as *Press Touch Finding Algorithm (PTFA)* with some modifications. One notable modification is that instead of finding a global optimum peak, the *PTFA* always has to discover local maximum peaks. Moreover, it also has to count the number of peaks since it is the *PTC* given by the user during the authentication session.

In the proposed scheme, a *brute-force* technique based *PTFA* is employed to discover all the local maximum peaks since the number of elements in ζ is considerably lower.

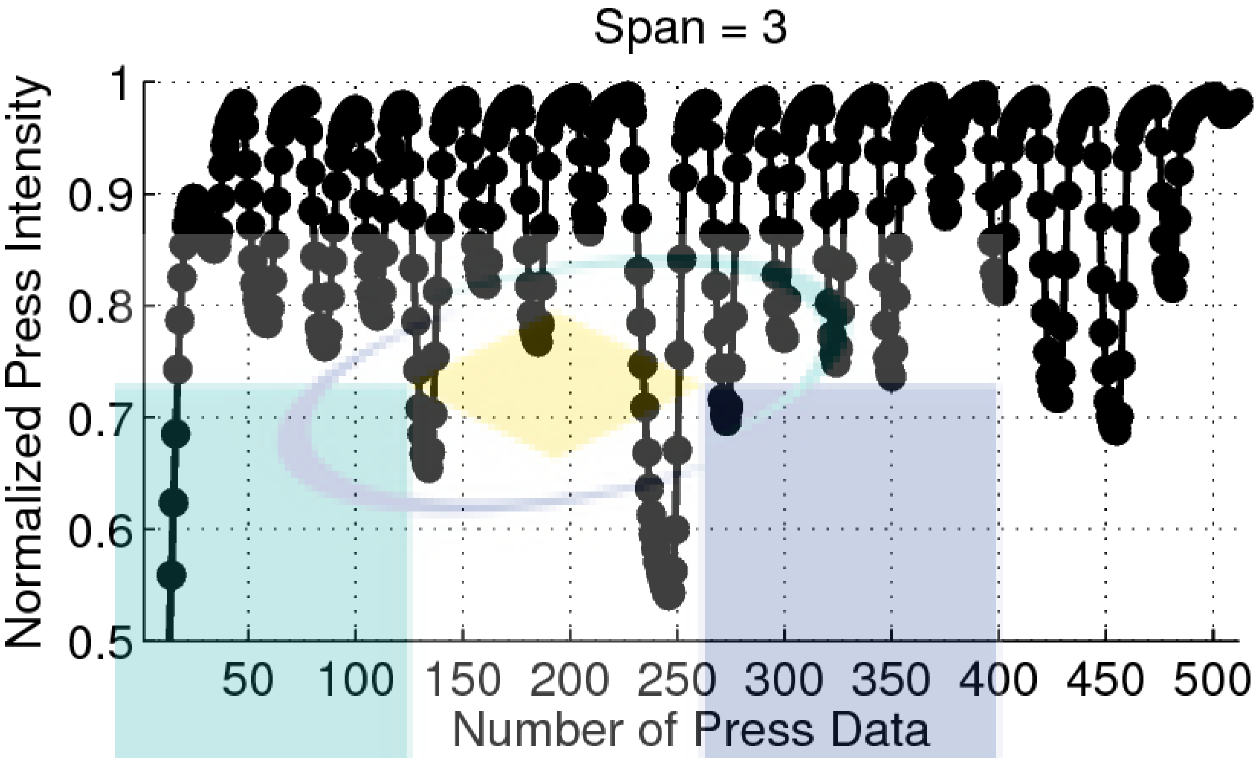

Figure 3.5. The acquired data after span 3

Other factor that influence to selecting *brute-force* technique is that it is simple to implement and requires comparable computational power when number of elements are lower like this scenario. Time complexity of this algorithm is $\mathcal{O}(n)$. In this algorithm, any press intensity value, ζ_{t_i} is a peak if it is greater than its neighbor(s), i.e.,

$$\zeta_{t_i-1} < \zeta_{t_i} > \zeta_{t_i+1} \qquad 3.2$$

where $\zeta_{t_0} = \zeta_{t_n+1} = -\infty$. Equation (3.2) is applied on ζ to discover all the local maximum peaks and as mentioned before, number of local maximum peaks are equivalent to number of *PT*s. For instance, in Figure 3.4, there are 20 local maximum peaks, which means that there are 20 *PT*s, i.e., $PTC = 20$. This value is then either store (in case of registration) as a signature of the particular user or compare (in case of authentication) with the registered signature to match the similarity. The pseudocode of this algorithm is detailed in Algorithm 1.

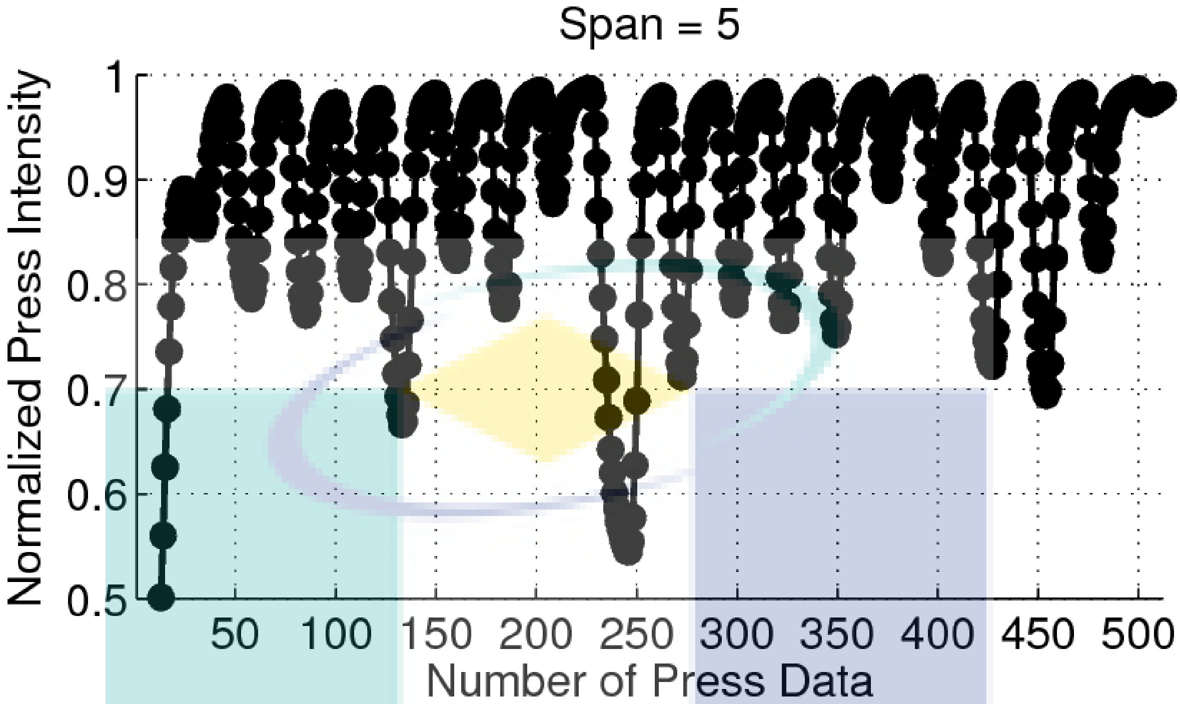

Figure 3.6. The acquired data after span 5

3.2.2 Multi-PTC

Although, it is possible to have a considerably large *PTC*; however, during the survey—detailed in Section 3.3.3—according to the observation, participants usually prefer moderate *PTC* values. Let's consider that the highest *PTC* provided by any user is μ. Hence, this is the highest achievable password space using *mono-PTC*. Such a small password space is not adequate to defend the *brute force* attack. However, password space can be enlarged by repeating the *mono-PTC* for several cycles. Thereby, the *mono-PTC* is extended with multiple cycles, named *multi-PTC*.

In *multi-PTC*, a user has to repeat *mono-PTC* for multiple cycles with an interval constraint. S/he has to repeat subsequent *mono-PTC* within a fixed time interval, τ. Again, τ must be cautiously selected since a large value of τ would result in a long authentication session and a smaller τ would result in expiration before starting the subsequent cycle. Both these τ values would reduce the usability of the proposed scheme. Long story short, a τ must be chosen reasonably small considering the usability issues of the user.

After completing one cycle of *PTC*, a user must start the subsequent cycle within the τ time unit. Conversely, it would be considered as the end of the authentication session. Since *PT*s are acquired in various cycles, a $2-D$ data structure, $\zeta_{t_{ij}}$ is employed to store press intensity values; where i is the index of a $1-D$ data structure, e.g., a vector like in *mono-PTC*, j is the index of the cycle, and $i, j \in \mathbb{Z}^+$. At the end of the data acquisition session, alike *mono-PTC*, all the data are cleaned using *MAFT* with $span = 3$. Afterwards, *PTFA* is

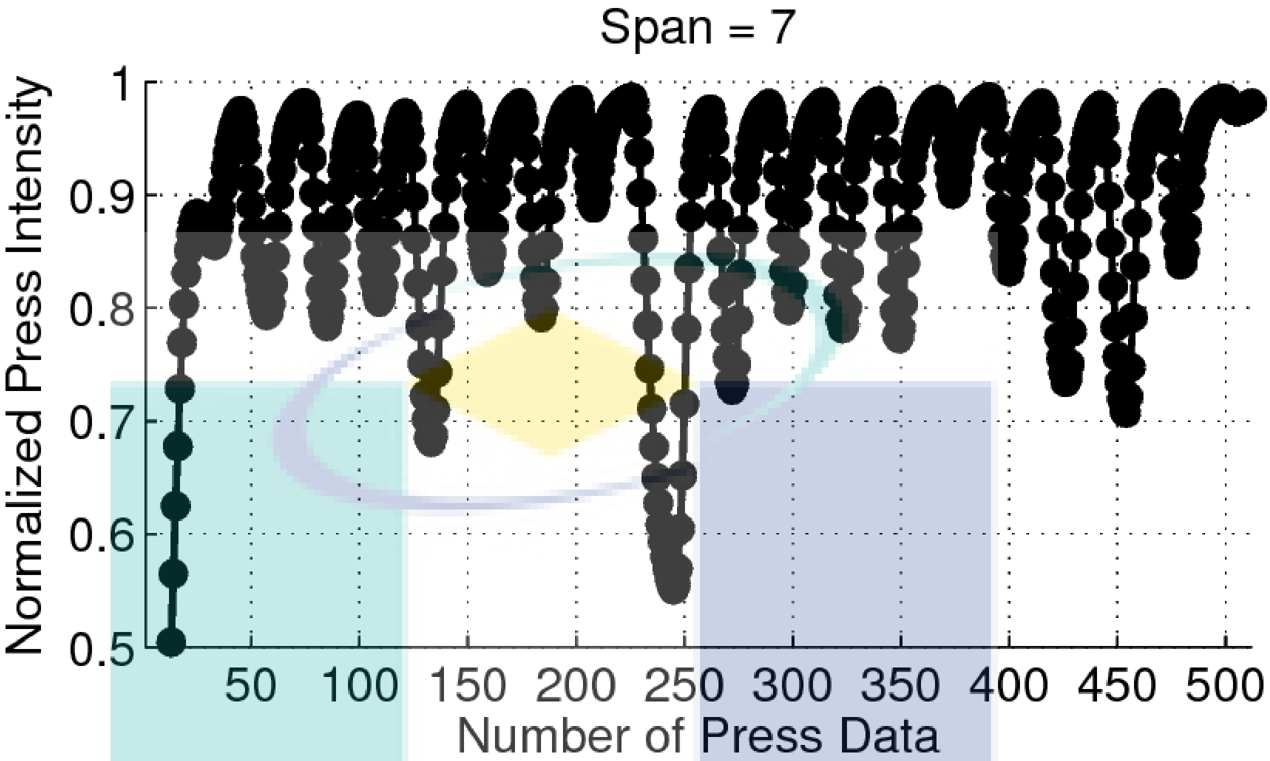

Figure 3.7. The acquired data after span 7

employed on every i to discover corresponding *PTC*, denoted as ρ_i. Every ρ_i is then stored in a vector, S; where $S = \{\rho_0, \rho_1, ..., \rho_m\}$ and m is the number of *PTC* giving cycles. In other words, S is the signature of the user, which s/he has to repeat during the authentication session. The password space of this scheme can be calculated as μ^m. For instance, when $\mu = 10$ and $m = 4$, it offers a password space equivalent to a 4-digit PIN, i.e., 10^4. That means, *multi-PTC* has affordable resilience against the *brute force* attack and it outperforms *mono-PTC* in this respect.

3.2.3 Multi-PTC with Grid

Although, *multi-PTC* offers an affordable resilience against *brute force* attack; however, it fails to ensure a high degree of resilience against such attack. Therefore, alike *Knock Code* (*LG V20 KNOCK ON AND KNOCK CODE*, 2017), *multi-PTC* is enhanced by incorporating a grid in it. For that a 2×2 grid is considered, i.e., four (4) cells ($C_{m,n}$), where m and n are row and column numbers, respectively; and $0 < m, n \leq 2$, as shown in Figure 3.8.

Algorithm 1 fPress Touch / Peak Finding Algorithm

```
$LocalPeakFound \leftarrow false$;
$TotalPeakFound \leftarrow 0$;
$Data[-1] \leftarrow -\infty$;
$Data[n] \leftarrow -\infty$;
for $i \leftarrow 0$ to $Data.size - 1$ do
    if $Data[i-1] \leq Data[i]$ && $Data[i] \geq Data[i+1]$ then
        $LocalPeakFound \leftarrow true$;
    else
        $LocalPeakFound \leftarrow false$;
    end if
    if $LocalPeakFound = true$ then
        $TotalPeakFound++$;
        $LocalPeakFound \leftarrow False$;
    end if
end for
    return $TotalPeakFound$;
```

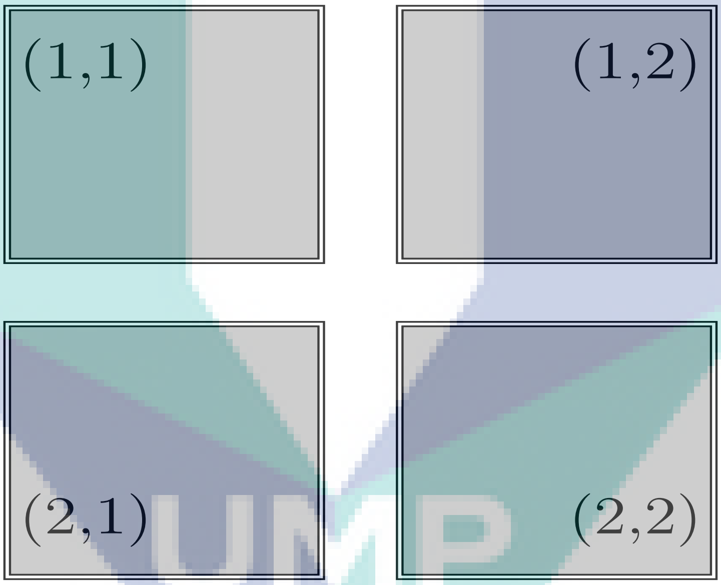

Figure 3.8. The 2×2 Grid for *multi-PTC with Grid* technique.

Unlike Android-based *Pattern Lock (PL)* scheme (Uellenbeck et al., 2013) (which utilizes a 3×3 grid), smaller grid is utilized to increase the usability and to fit the grid within the limited screen of the most smart devices. There are a couple of advantages of using a large cell area, such as: *i*) it is more convenient to press on a larger area than a smaller, *ii*) larger cells can resolve *fat-finger* problem, *iii*) increase the memorability, and *iv*) also assist the users with weak vision in using the system.

Every cell in the grid could be considered as a limited area for providing a *PTC*. A user can provide *PTCs* at multiple cells with repetitions. Even it can visit the same cell in consecutive cycles. Alike *multi-PTC*, τ plays an important role here. More specifically, suppose a user provide a *PTC* in $C_{1,1}$ and lifts his finger to provide another cycle of *PTC*. S/he has to start the next round within the τ time unit; otherwise, it would be considered as the end of the ongoing session. Again, from $C_{1,1}$, a user can choose any grid to provide his next cycle of *PTC*; even $C_{1,1}$ could be chosen. This freedom of choice resists this proposed technique from any *smudge* attack. The *PTCs* along with their cell information is jointly considered as a signature of that particular user and stored in a data structure (during registration phase) or is compared with the pre-registered signature (during authentication phase) to authenticate. Here, a pair, φ, is used to store the *PTC* of a particular cell and the identification number of that cell, i.e., $C_{m,n}$ and then, it is added in a multiset, ξ. Later, during the authentication phase, newly given multiset, ξ' is compared with the pre-registered multiset, ξ. The user will be given access if and only if $\xi' = \xi$.

Note that, in oppose to the *PTC* and *multi-PTC*, it is not suitable for miniature devices; and hence, not screen size independent. However, it works fine on any medium to large smart devices. Again, this variant is effective in the scenarios where *brute force* attack is frequent and there is no restriction in retrying. Otherwise, *multi-PTC* provides affordable resistance against such attacks.

3.2.4 Registration & Authentication

For utilizing the *multi-PTC* on a smart device, a user has to register a signature first. For that, the user has to launch the application. Afterwards, s/he has to place the finger within the given box on the screen as shown in Figure 3.2 and Figure 3.3 and has to provide *PT*s quickly and sharply. After finishing the first cycle, the user must lift the finger from the screen. If the user desires to provide another cycle of *PTC*, s/he has to start the procedure within the τ time unit as discussed in the Proposed Scheme Section. Following this procedure, the user can repeat the *PTC* as many numbers of cycles as s/he wants. Any interval, τ' more than τ, i.e., $\tau' > \tau$ would be considered as the end of the registration session. Later on, all the acquired data would be processed to extract the signature of the particular user and would be saved in *S*. The user can attempt to registrations as many times as possible until s/he is satisfied. Once the user is satisfied, s/he has to press the confirmation button; otherwise, press the repeat button. The entire registration and authentication procedure is illustrated using a flowchart in Figure 3.9 and Figure 3.10. In case of *multi-PTC with Grid*,

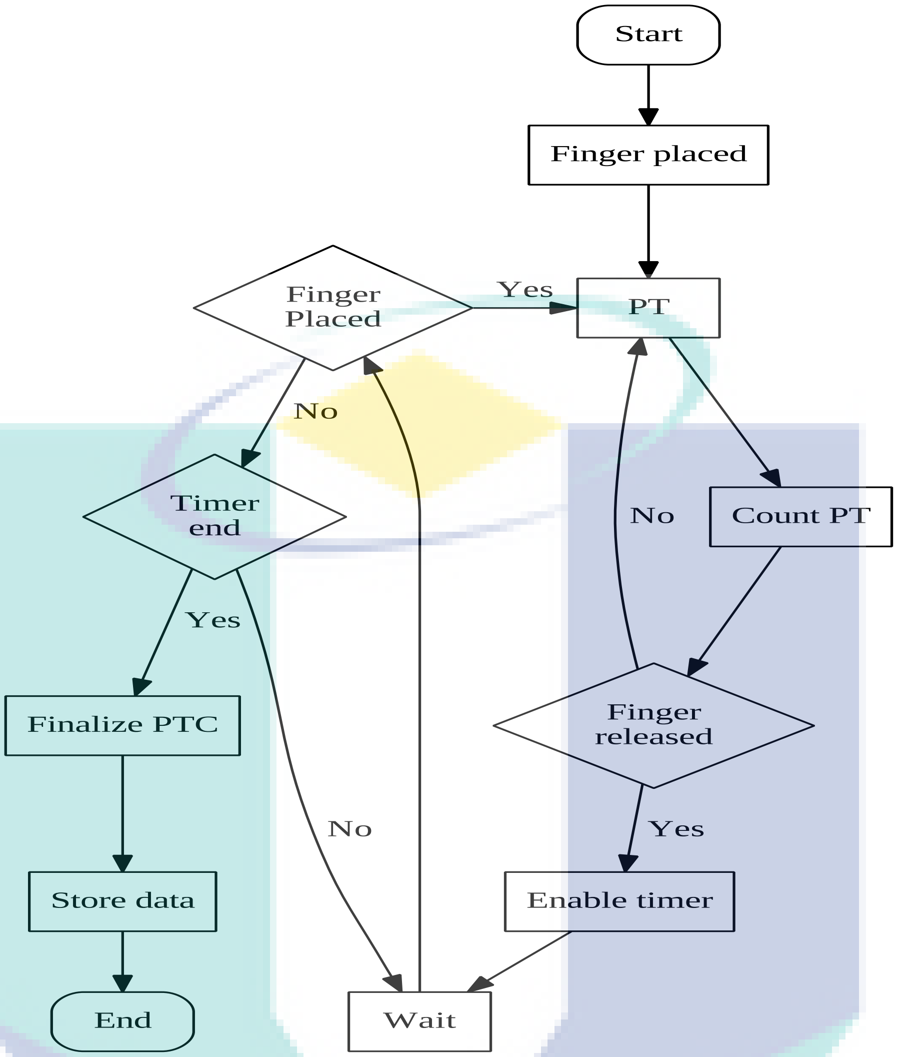

Figure 3.9. Flowchart of the registration phase of the *multi-PTC* variant

the registration procedure is similar to that of *multi-PTC* except *PTCs* must be provided on different cells instead of random places on the screen. Once a user is registered, the device locking system is enabled. Later on, to unlock the device, the user has to pass through an authentication session where s/he has to validate thyself by repeating the signature, which is provided during the registration session. This procedure is almost similar to the registration procedure, except the matching portion. Let's assume that the new signature provided by the user is S'. Now, the screen would be unlocked only when $S' = S$. Both these signatures would be considered equivalent only when following two conditions are true. At first, the cardinality of both the signatures is checked. If they are equivalent, i.e., $|S'| = |S|$, only then the second condition is checked. In the second condition, every vector in S' is compared with the corresponding vector in S. They are considered equivalent only if $\forall_i \rho'_i = \rho_i$. The authentication process is illustrated in more details using a flowchart in Figure 3.10. For *multi-PTC with Grid*, the procedure is same except the pre-registered ξ is compared with the newly provided ξ', and the screen would be unlocked only when $\xi' = \xi$.

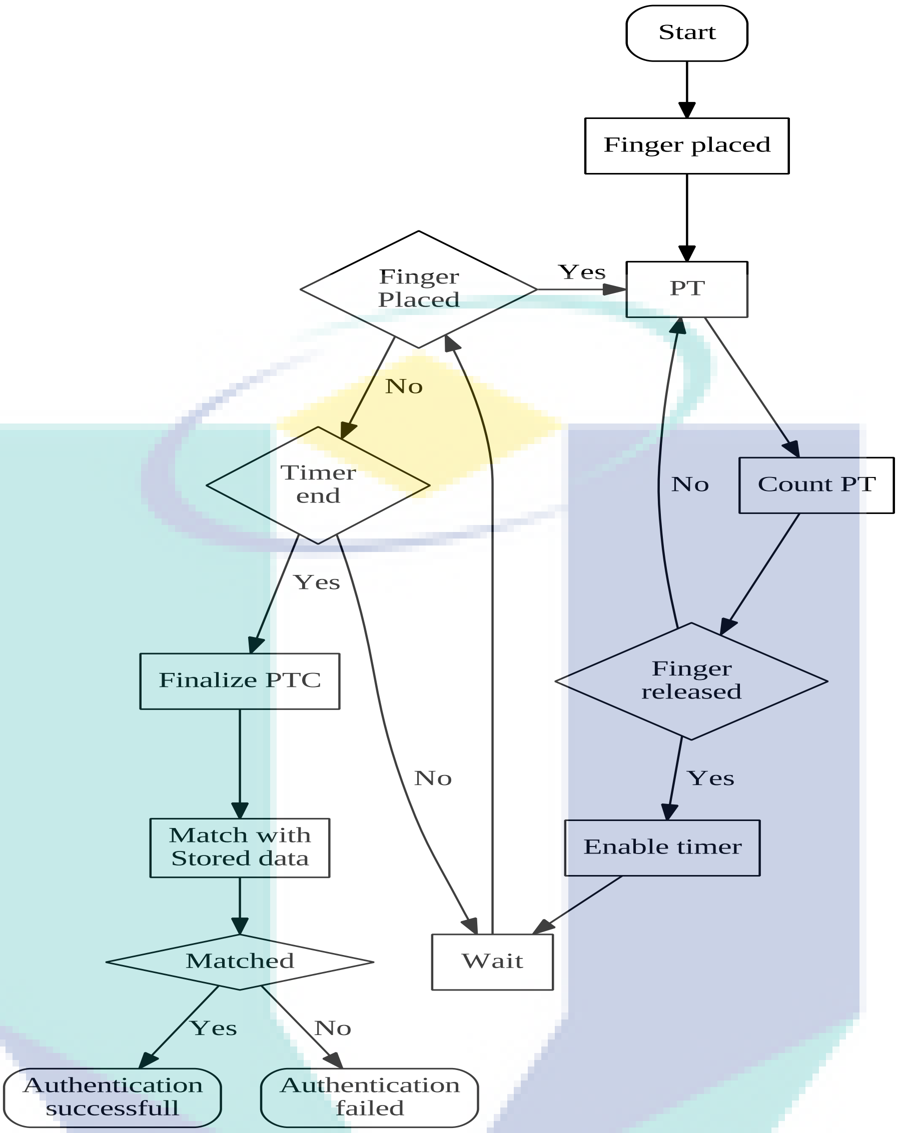

Figure 3.10. Flowchart of the authentication phase of the *multi-PTC* variant.

3.3 Evaluation setup

This subsection briefly describe the arrangements made for the evaluation of the proposed scheme. Initially the parameters for measuring performance is delineated, afterwards the experiment setup for *shoulder surfing* attack resilience evaluation is described, then detail of a survey setup for usability evaluation is given, which is done for the usability measurement of the proposed scheme.

3.3.1 Performance measurement parameter selection

Performance of the proposed scheme is measured based on several parameters, which are described bellow.

3.3.1.1 Attacks

Capability of resilience from certain attacks are taken as key parameters to measure the performance of the propose scheme, such as, *shoulder surfing* attack *smudge* attack, *brute force* attack.

***shoulder surfing* attack:** Where the intruder tries to attain the password of the user by staying close to him/her while he/she is performing registration or authentication. It also can be done by recording the user's authentication or registration session by hidden cameras.

***smudge* attack:** Where the attacker tries to identify a user's password by the oily residues or smudges, that remains on the screen for a certain time after a user enter his/her password.

***Brute force* attack:** Which is a trial-and-error based method, where an intruder tries to attain a user's password by a large amount of consecutive guesses, which is generated by an automated system.

3.3.1.2 Distance

To measure the *shoulder surfing* attack resilience, one of the key parameters is the distance. The possibility of such attack of the proposed schemes varies on the distance between the user and the intruder. A short distance between them increases the possibility of experiencing such attack.

3.3.1.3 Height

Height is considered as another important parameter to measure the resistance of the scheme against *shoulder surfing* attack. Even if the intruder is very close to the user, he/she has to espy from a certain height to acquire the password.

3.3.1.4 Screen size

To evaluate functionality of any *graphical* authentication scheme, screen size is a very essential key parameter. Screen size independent *graphical* authentication schemes are more effective and functional than the fixed size schemes.

3.3.1.5 Authentication duration

For functional measurement, authentication duration is another important parameter. Effective authentication schemes must not take long time for the authentication/registration.

On the other, authentication schemes that takes longer times fail to attain good usability ranking

3.3.1.6 Number of PTC

Preferred number of PTC by the average number of users is very important to measure the usability of the proposed scheme. If the number of PTC is high, the proposed scheme could be assumed adaptable and easy to use. On the other hand, the lower number of PTC indicates that, it is not decent enough to use. Again, it also increases the chances of *brute force* attack.

3.3.1.7 Memorability

Memorability is also an important parameter to measure the usability of the proposed scheme. Passwords of simple and easy schemes are more easy to memorize, where as, the password of complex schemes are difficult to memorize.

3.3.2 Experimental setup for finding shoulder surfing attack resilience:

In this experiment, videos of several authentication sessions are captured using a camera of both *multi-PTC* and *Knock Code* schemes by varying several parameters as shown in Figure 3.11. In details, a camera is set at: *i*) three different locations: 0.5m, 2m, and 3m, *ii*) two different heights: 1.5 m (eye level height of a mature man) and 2.5m (ceiling mounted camera height), and *iii*) three different directions: left, right, and front. In all the sessions, the camera was angled towards the smartphone. The ceiling mounted camera height was taken into account only for 3m distance since from that distance, it is difficult to discover any signature from eye level height (especially, both evaluating schemes). In every session—irrespective of the scheme—a random signature was registered and it was noted down on a paper for future reference. Throughout the whole experiment, a single right-handed male model was used. During the authentication session, the phone was kept horizontal to the ground so that with little efforts an attacker can acquire the signature. After capturing the videos of all the sessions, unnecessary parts are removed by video edit. Later on, the recorded videos are played to the participants and asked them to find out the signature for all the sessions. Note that only one chance was given to the participants to discover a signature. They noted down their answers on papers and returned them.

3.3.3 Survey setup for usability evaluation

An extensive survey is conducted on a good number of male and female smart phone users of different demographics to measure the usability of the proposed scheme, where every participant had to perform several tasks during the survey. They are discussed below:

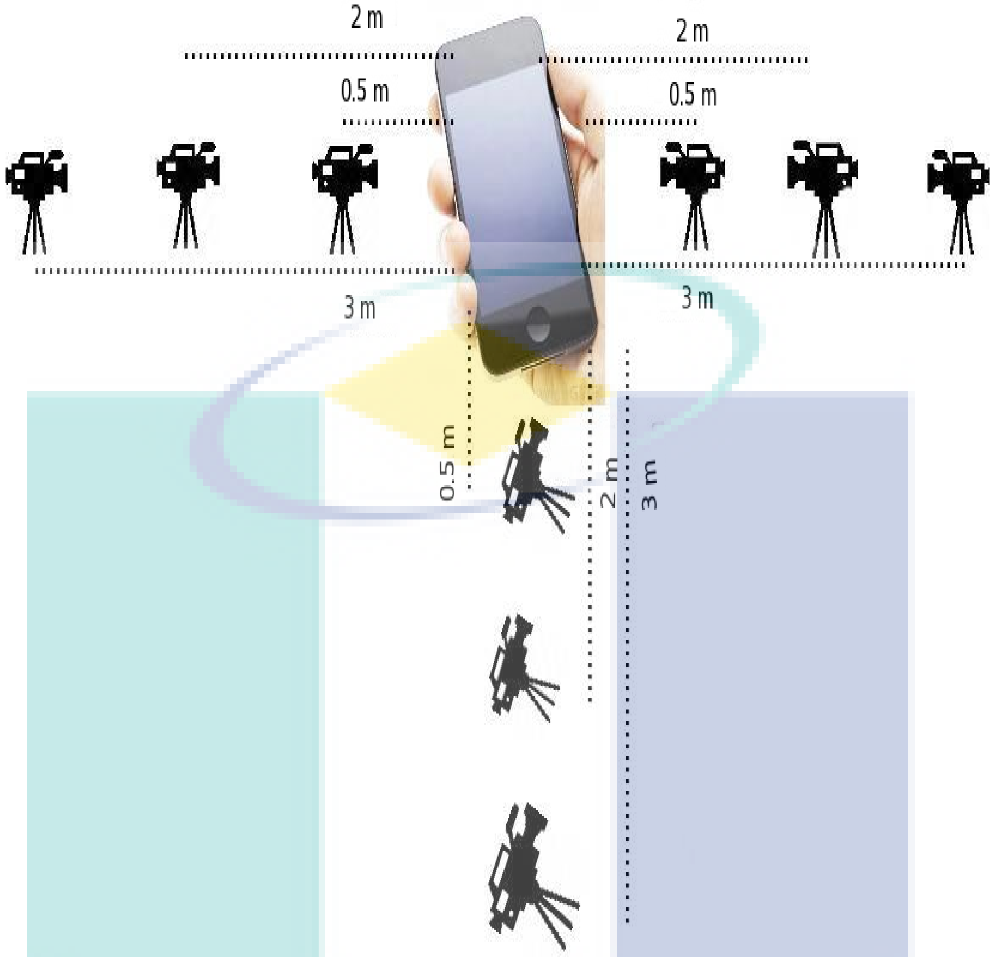

Figure 3.11. Experimental setup for discovering shoulder surfing attack on *multi-PTC* and *Knock Code*.

1. *Brief Introduction:* Since *PTC* is a new authentication scheme, it is necessary to make the participants familiar to the scheme. Therefore, before starting the survey, a brief introduction had been given to all the participants about the scheme, the registration procedure, the authentication procedure, and other related aspects.

2. *Registration:* At first, the system was launched to register a user as shown in Figure 3.9. According to the given instructions in the Proposed Scheme Section, a user can repeat until desire signature was registered. When the registration was complete, the user clicked the confirmation button; otherwise, clicked the repeat button to repeat the procedure.

3. *Authentication:* After completing the registration, the system was enabled and it locked the screen. Then after a considerable interval, the user was asked to unlock the screen by repeating the signature that was registered before. A detail description of the authentication procedure is given in the Proposed Scheme Section also shown in Figure 3.10. If the newly provided signature was matched with the previously registered signature, the screen was un-

locked. Otherwise, a user had to repeat the procedure. Although, in many systems, three consecutive unsuccessful retries are considered as an attempt to password breach; however, for the survey, this condition is not applied.

4. *Question & Answer Session:* After successfully completing the registration and authentication session, the users were asked various questions to acquire their feedbacks on the proposed scheme. All the answers were noted down and they were analyzed later.

3.4 Summary

This chapter elaborates the proposed novel technique—where a new code has been introduced by transforming the existing *Press Touch (PT)* technique of various smart devices, named *Press Touch Code (PTC)*. To enhance the security to a satisfactory level, Three variants of the proposed scheme are designed and implemented, namely *Mono PTC*, *Multi PTC*, and *Multi-PTC with Grid*. In *Mono PTC*, only one cycle of *PT* is taken from the user during the registration phase and in the authentication phase user has to repeat the code which is matched with the registered code to authenticate the user. *Multi PTC* is same as the *Mono-PTC*, but the code has to repeat multiple times. In case of *multi-PTC with Grid*, the registration procedure is similar to that of *multi-PTC* except PTCs must be provided on different cells instead of random places on the screen. An evaluation setup is also discussed in this chapter, where different parameters of evaluations are described elaborately. Description of an experimental setup to find the resilience against *shoulder surfing* attack of the proposed scheme and survey setup for usability testing is also included here.

CHAPTER 4

RESULTS AND DISCUSSIONS

4.1 Preamble

The proposed authentication scheme has been implemented on *Android Operating System* and tested on a *Huawei P9 Plus*, which is a *PST* enabled device. This application is suitable for any *Android* based device with similar specifications. To enable this application on other operating system requires necessary modifications. To evaluate the proposed scheme, an in-lab experiment is been conducted and a comprehensive survey on 105 male and female participants of different demographics. The design of the in-lab experiment and the survey had not violated any regulation of the university's Ethics Review Board. Prior to any experiment or any survey, a participant was asked to read and sign an informed consent form, which stated that his/her usability experience would be logged. In the form, a participant had to provide limited personal information so that later on it can be possible to trace back to him/her. Apart from that no personal information was accumulated neither during the experiment nor during the survey. Thus, all the data obtained were anonymous data. Therefore, no treatment was performed to de-identified them. Generally, any authentication scheme has three important requirements, namely security, functionality, and usability. Therefore, in this section, the proposed scheme is explained how it satisfies those requirements. In addition, this scheme can also be compared with other relevant prominent schemes to demonstrate the effectiveness of the proposed scheme.

4.2 Security Analysis

In this subsection, the strength of the proposed scheme against the *shoulder surfing*, *smudge*, and *brute force* attacks is analyzed. They are detailed below:

4.2.1 Shoulder Surfing Attack

To find out the resilience of the proposed scheme against *shoulder surfing* attacks, an in-lab experiment is performed and compares it with that of the *Knock Code* since it is the closest competitor of the proposed technique. The experimental setup is described in Chapter 3.

Table 4.1. Experimental results of *shoulder surfing* attack

Distance (m)	**multi-PTC**			**Knock Code**		
	Left	**Front**	**Right**	**Left**	**Front**	**Right**
0.5	0	0	0	0	0	0
2	0.37	0.5	0.875	0.37	0.5	0.67
3	0.625	0.95	0.75	0.125	0.1	0.615

All the results in Table 4.1 are computed based on the user feedbacks. As it could be observed from the table is that when the camera distance is near to the user, both the scheme has negligible or no defense against *Shoulder Surfing* attack. On the other hand, they attain certain levels of resilience for longer distances. Between both the schemes, *multi-PTC* outperforms its counterpart for all the parameters. One of the key reasons behind this is that presses are more sophisticated than knocks, and the latter could be recognized even from a long distance. Among the three directions, left side has the lowest *Shoulder Surfing* resilience over the other two sides for both the schemes. Since this model was right-handed, obviously he was holding the phone on the right hand, which exposed the left side and front side over right side. For that reason, at 2 m distance, right side has the most resilience against the *Shoulder Surfing* attack for both the schemes, i.e., 0.857 for *multi-PTC* and 0.67 for *Knock Code*. After interviewing several participants, this thesis revealed that many participants was also observing the hand movement to determine the number of knocks and presses. The *multi-PTC* attains the highest resilience for the distance of 3 m when the camera was at ceiling mounted height and the direction was front, which is 0.95; whereas, for the similar parameters, *Knock Code* performs poorly. The reason behind this is that knocks are recognizable even from a long distance, but the presses are seldom recognizable from that distance.

4.2.2 Brute force Attack

This kind of attack is possible on an authentication scheme when it offers a limited password space. In the proposed scheme, it can be found using Equation 4.1.

$$P = \mu^m \times N^m \qquad 4.1$$

where, μ is the highest allowable *PTC* in a single cycle, m is the number of *PTC* cycles, and N is the number of choices in cell selection. For instance, since in *mono-PTC*, the screen is not divided into cells, i.e., $N = 1$, and only one round of *PTs* is allowed, i.e., $m = 1$; P could be equivalent to μ only. If $\mu = 10$, then $P = \mu = 10$.

On the other hand, for *multi-PTC*, since it allows multiple cycles of *PTCs* and $N = 1$; P could be equivalent to μ^m. Therefore, when $\mu = 10$ and $m = 5$, it offers an equivalent password space to a 5-digit PIN, i.e., 10^5, which is greater than 4-digit PIN—a common authentication scheme of many smart devices.

Table 4.2. The password Space, P for three variants of the proposed scheme when $\mu = 10$ and $N = 4$

mono-PTC	m	mulit-PTC	multi-PTC with Grid
10	1	10	40
10	2	100	1600
10	3	1000	64000
10	4	10000	2560000
10	5	100000	102400000
10	6	1000000	4096000000
10	7	10000000	163840000000
10	8	100000000	6553600000000
10	9	1000000000	262144000000000

Again, in *multi-PTC with grid*, since the screen is divided into four (4) cells, a user would have four choices to provide his/her *PTC* in every cycle; and hence, it can offer a large password space, which is shown in Table 4.2 along with other two variants.

As it could be observed from the table is that *multi-PTC* offers an affordable resilience against the *brute force* attack by offering a considerably large password space for higher *m* values. However, it would fail to ensure a high degree of resilience when this kind of attack is frequent and no or limited password retrying policy is practiced. In such cases, *multi-PTC with Grid* would perform better due to offering a large password space even for moderate *m* values, which would take years to breach using the *brute force* attack.

4.2.3 Smudge Attack

The *Smudge* attack is another prominent attack on smart devices, which occurs due to oily residues or smudges that remain on the screen or on the surface of the device as a side effect of proving a password. Accumulating and analyzing these oily smudges are easily possible through sprinkling some powder like particles over the screen or even with a camera. A recent study found that it is possible to partially unlock a screen around 92% of cases, and fully in around 68% cases (Aviv et al., 2010).

Among all the variants of the proposed scheme, only *multi-PTC with Grid* has a possibility of experiencing such attack due to incorporating grid in the techique. However, since it permits a user to visit a cell multiple times, and thus, desponds all endeavors of an attacker to extract the information of visited cells.

4.3 Functional analysis

This section is emphasized on two functionalities that are closely related to the proposed scheme and its related schemes.

4.3.1 Screen size independence

Although, at present, there are many authentication schemes in operation; however, most of them are not screen size independent as mentioned in Chapter 1 and Chapter 2. This is one of the main motivations behind this work. For instance, most of the *textual* and *graphical* schemes are not screen size independent; specifically, they are not suitable for miniature smart devices. For *textual* schemes, they usually need a full or partial keyboard, which is not possible to fit in such devices. Again, for *graphical* schemes, a similar argument is appropriate since they also need to display some graphics on the screen. Among the three variants of the proposed scheme, *mono-PTC* and *mulit-PTC* are screen size independent, and could be applied on any sized smart devices.

4.3.2 Short authentication time

There exist some authentication schemes which offers higher securities, but takes a long time to authenticate; hence, are deemed not suitable for smart devices. For instance, *VAP Code* is a sense based technique that offers resilience against the *shoulder surfing*, *smudge*, and *brute force* attacks, but spends a large time in completing the authentication process. However, all three variants of the proposed scheme take considerably short times to authenticate.

4.4 Usability analysis

For evaluating the usability of the proposed scheme, an extensive survey was conducted 105 male and female participants of different demographics. This thesis targeted a varity of standard number of participants to get the usability of the scheme, thats why it choose 105 male and female participants, which will not produce a large data set but standard enough to justify the usability. All the participants had previous experience in using smart devices for a considerable length of time. During selecting participants, this research endeavor to keep the ratio equal between male and female. Due to the concern and effort, the difference between them is now negligible; hence, it is not highlighted. datas are collected through observation of the participants' interaction with the system as well as through asking several questions to the participants. this thesis opted for an in-person study for two reasons: *i*) since *PTC* requires a specific type of devices and it would be impractical to assume that all the participants have the device; and *ii*) conducting an in-person study allowed to observe the user behavior directly. Survey setup and tasklist of participants are detailed in Chapter 3.

This section presents the results that are acquired during the survey. To evaluate the usability of the proposed scheme, this research consider two metrics, they are: *i*) memorability and *ii*) preferred *PTC*. Memorability is the metric which measures the quality or state of being easy to remember. Although, this proposed scheme is new, more than 70% participants were able to unlock the screen within 2 attempts; whereas, more than 90% participants were able to unlock within 3 attempts. Among the others, who needed more than 3 attempts were mostly because of insincerities during the registration phase. The survey results of memorability metric are depicted in Figure 4.1,

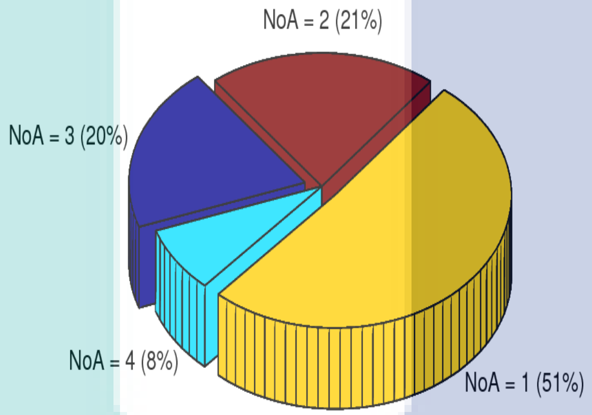

Figure 4.1. Memorability of the proposed technique. Here, *NoA* stands for *Number of Attempts*.

where *NoA* stands for *Number of Attempts*. All the users were able to do the registration and authentication without any difficulty, which portrays the easiness of using the system. Figure 4.2 shows the percentile results of preferred *PTC* selection during the registration phase. As it could be seen in the figure is that around 55% participants prefer *PTC*s more than 4; whereas, in *VC* (Azad et al., 2016), only 19% participants prefer to provide *VC*s more than 4. It is because of convenience in *PT*s over sensing vibrations. The longer registration and authentication time is another factor which lowers the count for the *VC*. In compare to *Knock Code*, since during a single *PTC* giving cycle, a user does not have to lift the finger from the screen; it is more convenient than the counterpart where it is just opposite. Overall, the majority admitted,the proposed technique is very easy and straightforward.

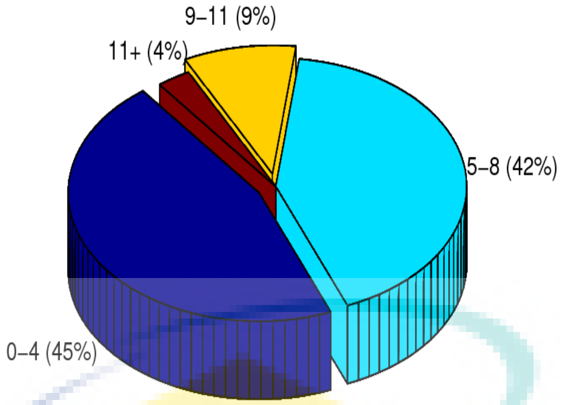

Figure 4.2. Preferred *PTC* of the proposed technique.

4.5 Comparison with related schemes

In this section, the proposed scheme is compared with other prominent related schemes. It is performed in terms of resistance and functionality. For this, this thesis take five prominent related schemes into consideration along with the three variants of the proposed schemes, namely *PIN* (Murdoch, Drimer, Anderson, & Bond, 2010), *AlphaNumeric (AN)* (Nayak & Bansode, 2016), *Android Pattern Lock (APL)* (Kwon & Na, 2014), *VAP Code (VAPC)* (Azad et al., 2016), and *Knock Code (KC)* (*LG V20 KNOCK ON AND KNOCK CODE*, 2017).

Table 4.3. Comparison of prominent related schemes with the three variants of the proposed scheme

.

Attack/Function	**PIN**	**AN**	**APL**	**VAPC**	**KC**	**mono-PTC**	**multi-PTC**	**multi-PTC with Grid**
Shoulder surfing	H	H	H	L	M	LM	LM	LM
Brute force	H	M	M	L	L	H	M	L
Smudge	M	M	H	L	L	L	L	L
Screen Size Independence	N	N	N	N	Y	Y	Y	N
Short Authentication Time	Y	Y	Y	N	Y	Y	Y	Y

*Legends: L - Low, LM - Lower Medium, M - Medium, H - High , N - No, Y - Yes.

Table 4.3 lists the resistance and functionality comparison of prominent related schemes along with the three variants of the proposed scheme. As could be observed from the table is that *PIN*, *AN*, and *APL* schemes are vulnerable to *shoulder surfing*, *brute force*, and *smudge* attacks in the range of medium to high which are argued previously in section 2.5. On the other hand, *VAPC* and *KC* have resistance from low to medium for those attacks, which is also debated in section 2.5. Again, all the three variants of the proposed scheme offer low to lower medium resistance for the *shoulder surfing* and *Smudge* attacks. However, in case of the *brute force* attack, *mono-PTC* has high vulnerability, *multi-PTC* has medium vulnerability, and *multi-PTC with Grid* has low vulnerability. Again, from the table, it could be observed that most of the schemes are not screen size independent. Only *KC*, *mono-PTC*, and *multi-PTC* could be applied also in miniature devices. From the above discussions, a conclusion can be made that *VAPC* and *KC* are the closest competitor of the proposed scheme.

Although *VAPC* offers the high degree of resilience against three prominent attacks (Azad et al., 2016) that are taken into account in this comparison; however, it is not screen size independent and takes a long time during authentication phase as demonstrated in Chapter 2 with an example. On the other hand, all the variants of the proposed scheme are more resilient against *shoulder surfing* attacks than *KC*, which is demonstrated in Section 4.2.1 by performing an experiment. Consequently, if the trade-off among all the related schemes is considered in terms of resistance and functionality, this proposed scheme has better efficiency than others.

4.6 Validity threats

Several validity threats can be associated with the in-lab experiment and the survey that have conducted. Among them, significant threats are identified and mentioned below along with the steps that have taken into account to mitigate them on the acquired results.

- Firstly, the choice of the device poses an essential threat since there are several other devices available in the market with the similar specifications. Note that, this proposed scheme has been implemented and tested on the Huawei P9 Plus device as mentioned earlier. However, in favor of the selection of the device,this thesis would like to argue that the press intensity value has been acquired by calling an *Android* function, which is device independent. Therefore, this proposed scheme is applicable on any *PST* enabled *Android* device. On the other hand, it requires a considerable amount of modifications in terms of implementation to adopt to other *PST* enabled devices with different operating system.

- Secondly, data acquisition from a fixed box or area on the screen is another important threat. This thesis utilize this box to expel any confusion that may arise in deciding where to press. Again, this research have opted this since from the investigation, this research discover that—irrespective of the area—a *PT* provides similar haptic feedback and elicit a similar set of responses depending on the intensity of the press. Hence, this thesis would like to argue that the press intensity values would not differ due to changing or expanding the data acquisition area.

- Thirdly, the parameters those have been chosen to conduct the experiment are indispensable threats, because any parameter tuning may produce a different set of results. However, in the experimental setup, the parameters were selected in such a way that they may bring off the vulnerabilities of both the tested schemes (i.e., *Knock Code* and *multi-PTC*) without favoring any one of them. For instance, during all the experiments, the device was kept horizontal to the ground since it is the most vulnerable position for the *Shoulder Surfing* attack. Any change in the position would result in higher defense against the attack for both the schemes.

Again, instead of field-based experiments, lab-based experiments are conducted where videos are recorded of various authentication sessions. Later on, all of them are played on a standard laptop monitor to the participants and acquired their feedbacks. Again, to bring off the vulnerabilities of both the schemes, such setup is adopted. During a filed-based experiment, several environmental factors (such as movement, conversation, light, and so on) would influence the results; whereas, in lab-based experiments, those were absent. Therefore, the participants were able to recognize the signatures oftenly for various parameters.

- Fourthly, in the survey, only those participants are selected who have a considerable duration of experiences in using smart devices, which also could be considered as a threat. However, this thesis would like to lay following arguments in favor of the selection: *i*) experience users would require minimum briefing to introduce the proposed scheme, *ii*) experience participants would spend lower time in registration and authentication than others, and *iii*) they could give more productive suggestions and feedbacks, which would later assist in improving the scheme.

- Finally, the choices of performance metrics for evaluating the effectiveness of the proposed scheme can also pose as threats. In this case, although two metrics are considered, namely *i*) memorability and *ii*) preferred *PTC*; but other metrics also exist. Among the selected metrics, memorability is a well-known and well-established metric that tells the easiness in remembering a scheme. Any complex scheme may increase the security of the system, but people would only embrace this scheme if it is easy to remember. Hence, the choice of this metric is appropriate. Again, the second metric is related to the proposed scheme, which is necessary to understand user behavior in providing the *PTC*.

4.7 Summary

This Chapter analysis the performance of the proposed scheme based on three different parameters, namely, security analysis, functional analysis and usability analysis. In the security analysis, the proposed scheme is tested by, *shoulder surfing* attack, *brute force* attack and *smudge* attack, where the proposed scheme shown an acceptable resilience against each attack. In functional analysis, it is shown that the scheme is functional in any size of screen, which is one of the main nobality of this scheme, where most of the existing authentication schemes do not have this dynamic feature. Another advantage of this scheme is enlighten here, which is-completing authenticating/registration with a short period of time. In the usability analysis, an extensive survey is performed with a 105 participants. The responses from the participants are also analyzed and found positive; and they admit that the proposed scheme is easy to use. Afterwards, the scheme is compared deeply with the most relavent authentication schemes based on different parameters. In most case, the proposed scheme is found effective than the other related schemes. At the end, the validity threats of proposed scheme are discussed briefly.

CHAPTER 5

CONCLUSIONS

5.1 Preamble

This thesis propose, a novel screen size independent authentication scheme, which is implemented and tested according to the design, on an Android OS based environment. Then an in-lab experiment is performed to discover the *Shoulder Surfing* attack resilience of the proposed scheme and an extensive survey is conducted to evaluate the usability of it. At the end, contributions, limitations and the future work are discussed, following by a brief summary of the entire research.

5.2 Concluding Remarks

In this thesis, the first objective is to design a novel screen size independent authentication scheme, which would offer an affordable defense against the *shoulder surfing* attack. To achieve that objective, a novel authentication scheme is designed and implemented, which transforms the *PT* of the *PST* enabled smart devices to a code, named *PTC*. Two variants of the proposed scheme are introduced, namely *mono-PTC* and *multi-PTC*. They are screen size independent and also offer resilience against the *Shoulder Surfing* and *smudge* attacks. However, in terms of, the *brute force* attack, since *mono-PTC* offers a limited password space; hence, it is more vulnerable than the other. Conversely, *multi-PTC* offers an affordable defence against such attack by allowing a user to repeat *PTC* for multiple cycles.

To offer a higher degree of security from *smudge* and *brute force* attacks, which is the second objective of this thesis, the proposed authentication scheme is enhanced by integrating grid cells into it, called *multi-PTC with Grid*. Although, it has resilience against all three prominent attacks mentioned earlier, but it is not screen size independent. The proposed scheme is evaluated using an in-lab experiment and a comprehensive survey on 105 male and female participants. The experiment shows that the proposed scheme offers a higher resilience against *Shoulder Surfing* attack over the *Knock Code*. The responses from the participants are also analyzed and found positive; and they admit that the proposed scheme is easy to use. The proposed scheme is evaluated with five prominent related schemes in terms of resistance and functionality. From the comparison, it can be concluded that the proposed scheme is more efficient than others due to offering better trade-off.

5.3 Contributions

The main contributions of the thesis are described bellow:

1. Initially, a novel screen size independent authentication scheme is introduced, where the Press Touch (PT)—a.k.a., Force Touch in Apples MacBook, Apple Watch, ZTEs Axon 7 phone; 3D Touch with iPhone 6 and 7; and so on—is transformed into a new type of code, named Press Touch Code(PTC). After that mono-PTC, multi-PTC are designed and implemented based on PTC on the Android OS, which offers an affordable defense against the *shoulder surfing* attack.

2. To strengthen the security, the proposed authentication scheme is enhanced by integrating grid cells in it to attain resilliance against the *smudge* attack and the *brute force* attack, which is named as *multi-PTC with Grid*.

5.4 Limitations

Although the proposed scheme is effective, screen size independent, and offers resilience against three prominent attacks (namely, *shoulder surfing* attack, *brute force* attack, and *smudge* attack), still it has some limitations, such as.

1. Although, the *mono-PTC* and the *multi-PTC* are screen size independent and also offer an affordable defence against the *shoulder surfing* attack, but this scheme do not have a strong defence against the *brute force* attack.

2. Again, although the enhanced scheme, *multi-PTC with grid*, has resilience against the *brute force* and the *smudge* attack, but still it is not screen size independent. Moreover, it takes a considerable long time for authentication/registration.

5.5 Future works

This work lays the foundation for a screen size independent authentication scheme. It also introduced the use of *PST* display in a authentication schemes. The next upgradation of these scheme can be done by integrating biometric pattern recognition. A novel biometric scheme can be proposed using press touch characteristics of human being and incorporate it with the former scheme. This scheme will fall under the class of behavioral biometric. For recognizing the patterns of various individuals, various parameters can be taken into account, namely various angels at the top and at the bottom, intensity of the press, amplitude of the press, peaks, valleys, frequency of presses, and so on. Afterwards, these parameters can be used to identify someone with the help of *Neural Network* (Demuth, Beale, De Jess, & Hagan, 2014), which work on trial and error basis, where a system is taught by a specific algorithm to recognize any specific items even if they come up with different attributes. Likewise in this case, the PT of every individual will definitely not the same every time. Therefore, *Neural network* will be a good choice where different set of PT data can be fed into the algorithm to train the system to recognize specific individual properly. Since analyzing users' PT pattern is a novel approach, so this thesis can not desire to get 100% recognition by the system. Therefore, fuzzy technique can be used by arranging the data set according to fuzzy set and can be using *Fuzzy logic* (Klir & Yuan, 1995) to set the threshold value.

5.6 Summary

This section concludes the thesis by giving a brief summary of the entire research. The contributions of the thesis are discussed, where the three variants of the proposed schemes and the comparison of the proposed scheme with other existing authentication schemes are enlightened. Afterwards, the limitations of the proposed scheme are detailed, such as, a device must have a *PST* enabled display, and so on. The chapter ends by giving a vision for the future works, where some hints are given; how a the proposed scheme can be transformed into a biometric based authentication scheme using *Neural Networks* and *Fuzzy logics*.

REFERENCES

Abdullah, M. D. H., Abdullah, A. H., Ithnin, N., & Mammi, H. K. (2008). Towards identifying usability and security features of graphical password in knowledge based authentication technique. In Modeling & simulation, 2008. aicms 08. second asia international conference on (pp. 396–403).

Andriotis, P., Tryfonas, T., & Oikonomou, G. (2014). Complexity metrics and user strength perceptions of the pattern-lock graphical authentication method. In International conference on human aspects of information security, privacy, and trust (pp. 115–126).

Andriotis, P., Tryfonas, T., Oikonomou, G., & Yildiz, C. (2013). A pilot study on the security of pattern screen-lock methods and soft side channel attacks. In Proceedings of the sixth acm conference on security and privacy in wireless and mobile networks (pp. 1–6).

Authentication, R. U. P. (2004). The science behind passfaces. White Paper, June.

Aviv, A. J., Gibson, K. L., Mossop, E., Blaze, M., & Smith, J. M. (2010). Smudge attacks on smartphone touch screens. Woot, 10, 1–7.

Azad, S., Rahman, M., Ranak, M. N., Ruhee, B. K., Nisa, N. N., Kabir, N., Zain, J. M. (2016). Vap code: A secure graphical password for smart devices. Comput-ers & Electrical Engineering.

Bellare, M., Pointcheval, D., & Rogaway, P. (2000). Authenticated key exchange secure against dictionary attacks. In Advances in cryptologyeurocrypt 2000 (pp. 139– 155).

Bianchi, A., Oakley, I., Kostakos, V., & Kwon, D. S. (2011). The phone lock: au-dio and haptic shoulder-surfing resistant pin entry methods for mobile devices. In Proceedings of the fifth international conference on tangible, embedded, and embodied interaction (pp. 197–200).

Blackburn, D., Miles, C., Wing, B., & Shepard, K. (2007). Biometrics overview. National Science and Technology Council (NSTC) Committee on Technology Com-mittee on Homeland and National Security.

Blonder, G. E. (1996). Graphical password, us patent 5559961. September.

Bond, M., & Zielinski, ´P. (2003). Decimalisation table attacks for pin cracking (Tech. Rep.). University of Cambridge, Computer Laboratory.

Brostoff, S., & Sasse, M. A. (2000). Are passfaces more usable than passwords? a field trial investigation. In People and computers xivusability or else! (pp. 405–424). Springer.

Chang, Y. F., Chen, C., & Zhou, H. (2009). Smart phone for mobile commerce. Computer Standards & Interfaces, 31(4), 740–747.

Cormen, T. H., Leiserson, C. E., Rivest, R. L., & Stein, C. (2001). Introduction to algorithms second edition. The MIT Press.

Davies, J. (1999). Visual code recordal and communication thereof international patent pct. GB1999/001688.

Davis, D., Monrose, F., & Reiter, M. K. (2004). On user choice in graphical password schemes. In Usenix security symposium (Vol. 13, pp. 11–11).

De Angeli, A., Coventry, L., Johnson, G., & Renaud, K. (2005). Is a picture really worth a thousand words exploring the feasibility of graphical authentication systems. International Journal of Human-Computer Studies, 63(1), 128–152.

De Luca, A., Langheinrich, M., & Hussmann, H. (2010). Towards understanding atm security: a field study of real world atm use. In Proceedings of the sixth symposium on usable privacy and security (p. 16).

De Luca, A., Von Zezschwitz, E., Nguyen, N. D. H., Maurer, M.-E., Rubegni, E., Scip-ioni, M. P., & Langheinrich, M. (2013). Back-of-device authentication on smart-phones. In Proceedings of the sigchi conference on human factors in computing systems (pp. 2389–2398).

Demuth, H. B., Beale, M. H., De Jess, O., & Hagan, M. T. (2014). Neural network design. Martin Hagan.

Dhamija, R., & Perrig, A. (2000). Deja vu-a user study: Using images for authentication. In Usenix security symposium (Vol. 9, pp. 4–4).

Ding, Y., & Horster, P. (1995). Undetectable on-line password guessing attacks. ACM SIGOPS Operating Systems Review, 29(4), 77–86.

Dirik, A. E., Memon, N., & Birget, J.-C. (2007). Modeling user choice in the passpoints graphical password scheme. In Proceedings of the 3rd symposium on usable pri-vacy and security (pp. 20–28).

Dunphy, P., Nicholson, J., & Olivier, P. (2008). Securing passfaces for description. In Proceedings of the 4th symposium on usable privacy and security (pp. 24–35).

Dunphy, P., & Yan, J. (2007). Do background images improve draw a secret graphical passwords? In Proceedings of the 14th acm conference on computer and communications security (pp. 36–47).

Gao, H., Jia, W., Ye, F., & Ma, L. (2013). A survey on the use of graphical passwords in security. JSW, 8(7), 1678–1698.

Goyal, V., Kumar, V., Singh, M., Abraham, A., & Sanyal, S. (2005). Compchall: addressing password guessing attacks. In Information technology: Coding and computing, 2005. itcc 2005. international conference on (Vol. 1, pp. 739–744).

History of the iphone 2007-2017: the journey to iphone x. (n.d.). Retrieved from https://www.t3.com/features/a-brief-history-of-the-iphone

Huawei. (n.d.). Huawei P9 Plus. Retrieved from lastaccessedin2017Jan;url: http://consumer.huawei.com/en/mobile-phones/mateS/index.htm

Hudgens, G. A., Fatkin, L. T., Billingsley, P. A., & Mazurczak, J. (1988). Hand steadiness: effects of sex, menstrual phase, oral contraceptives, practice, and handgun weight. Human factors, 30(1), 51–60.

Janczewski, L. J., & Fu, L. (2010). Social engineering-based attacks: Model and new zealand perspective. In Computer science and information technology (imcsit), proceedings of the 2010 international multiconference on (pp. 847–853).

Jansen, W. (2004). Authenticating mobile device users through image selection. WIT Transactions on Information and Communication Technologies, 30.

Jermyn, I., Mayer, A. J., Monrose, F., Reiter, M. K., Rubin, A. D., et al. (1999). The design and analysis of graphical passwords. In Usenix security (pp. 1–14).

Karnan, M., Akila, M., & Krishnaraj, N. (2011). Biometric personal authentication using keystroke dynamics: A review. Applied Soft Computing, 11(2), 1565–1573.

Kim, I. (2012). Keypad against brute force attacks on smartphones. IET Information Security, 6(2), 71–76.

Klein, D. V. (1990). Foiling the cracker: A survey of, and improvements to, password security. In Proceedings of the 2nd usenix security workshop (pp. 5–14).

Klir, G., & Yuan, B. (1995). Fuzzy sets and fuzzy logic (Vol. 4). Prentice hall New Jersey.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineer-ing attacks. Journal of Information Security and applications, 22, 113–122.

Kwon, T., & Na, S. (2014). Tinylock: Affordable defense against smudge attacks on smartphone pattern lock systems. computers & security, 42, 137–150.

Lane, E. W., & Poole, E. S. (1883). The thousand and one nights: commonly called, in england, the arabian nights' entertainments (Vol. 1). Chatto and Windus.

Lashkari, A. H., Farmand, S., Zakaria, D., Bin, O., Saleh, D., et al. (2009). Shoulder surfing attack in graphical password authentication. arXiv preprint arXiv:0912.0951.

Lashkari, A. H., Saleh, R., Towhidi, F., & Farmand, S. (2009). A complete comparison on pure and cued recall-based graphical user authentication algorithms. In Computer and electrical engineering, 2009. iccee'09. second international conference on (Vol. 1, pp. 527–532).

Lg v20 knock on and knock code. (2017). Retrieved from http://www.lg.com/us/support/product-help/CT10000025-20150217113217-activation

Lin, D., Dunphy, P., Olivier, P., & Yan, J. (2007). Graphical passwords & qualitative spatial relations. In Proceedings of the 3rd symposium on usable privacy and security (pp. 161–162).

Matyas, S. M., & Stapleton, J. (2000). A biometric standard for information management and security. Computers & Security, 19(5), 428–441.

McGing, B. C. (2010). Polybius' histories. Oxford University Press.

Mihailescu, P. (2007). The fuzzy vault for fingerprints is vulnerable to brute force attack. arXiv preprint arXiv:0708.2974.

Morris, R., & Thompson, K. (1979). Password security: A case history. Communications of the ACM, 22(11), 594–597.

Murdoch, S. J., Drimer, S., Anderson, R., & Bond, M. (2010). Chip and pin is broken. In Security and privacy (sp), 2010 ieee symposium on (pp. 433–446).

Nayak, A., & Bansode, R. (2016). Analysis of knowledge based authentication system using persuasive cued click points. Procedia Computer Science, 79, 553–560.

Neuman, B. C., & Ts'o, T. (1994). Kerberos: An authentication service for computer networks. IEEE Communications magazine, 32(9), 33–38.

Owens, J., & Matthews, J. (2008). A study of passwords and methods used in brute-force ssh attacks. In Usenix workshop on large-scale exploits and emergent threats (leet).

Pareek, N., Patidar, V., & Sud, K. (2005). Cryptography using multiple one-dimensional chaotic maps. Communications in Nonlinear Science and Numerical Simulation, 10(7), 715–723.

Perkins, D. N. (1979). Your memory: How it works and how to improve it by kenneth l. higbee, the psychology of memory by alan d. baddeley (review). Leonardo, 12(1), 72–73.

Pinkas, B., & Sander, T. (2002). Securing passwords against dictionary attacks. In Proceedings of the 9th acm conference on computer and communications security (pp. 161–170).

Por, L., & Lim, X. (2008). Multi-grid background pass-go. WSEAS Transactions on Information Science and Applications, 7(7), 1137–1148.

Por, L. Y., Lim, X., Su, M., & Kianoush, F. (2008). The design and implementation of background pass-go scheme towards security threats. WSEAS Transactions on Information Science and Applications, 5(6), 943–952.

Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001). An analysis of minutiae matching strength. In International conference on audio-and video-based biometric person authentication (pp. 223–228).

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

Smith, S. W., et al. (1997). The scientist and engineer's guide to digital signal process-ing.

Snell, B. (2016). Mobile threat report: Whats on the horizon for 2016. Intel Security and McAfee, published March, 1.

Song, Y., Cho, G., Oh, S., Kim, H., & Huh, J. H. (2015). On the effectiveness of pattern lock strength meters: Measuring the strength of real world pattern locks. In Proceedings of the 33rd annual acm conference on human factors in computing systems (pp. 2343–2352).

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

Take advantage of 3d touch. (n.d.). Retrieved from www.developer.apple.com/ios/3d-touch/

Tao, H., & Adams, C. (2008). Pass-go: A proposal to improve the usability of graphical passwords. IJ Network Security, 7(2), 273–292.

Tari, F., Ozok, A., & Holden, S. H. (2006). A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords. In Proceedings of the second symposium on usable privacy and security (pp. 56–66).

Thorpe, J., & van Oorschot, P. C. (2004). Towards secure design choices for implementing graphical passwords. In Computer security applications conference, 2004. 20th annual (pp. 50–60).

Total, S. U. W. W. (2014). 1.75 billion in 2014. Mobile users pick up smartphones as they become more affordable, 3G and 4G networks advance.

The touching history of touchscreen tech. (n.d.). Retrieved from https://mashable.com/2012/11/09/touchscreen-history/#90NRKF4tTsqU

Towhidi, F., & Masrom, M. (2009). A survey on recognition based graphical user authentication algorithms. arXiv preprint arXiv:0912.0942.

Uellenbeck, S., Durmuth, ¨M., Wolf, C., & Holz, T. (2013). Quantifying the security of graphical passwords: the case of android unlock patterns. In Proceedings of the 2013 acm sigsac conference on computer & communications security (pp. 161–172).

Valentine, T. (1998). An evaluation of the passface personal authentication system. Technical Report, Goldsmiths College.

Valentine, T. (1999). Memory for passfaces after a long delay (Tech. Rep.). Technical Report, Goldsmiths College, University of London.

Viehbock, ¨S. (2011). Brute forcing wi-fi protected setup. Wi-Fi Protected Setup, 9.

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).

Von Zezschwitz, E., Koslow, A., De Luca, A., & Hussmann, H. (2013). Making graphic-based authentication secure against smudge attacks. In Proceedings of the 2013 international conference on intelligent user interfaces (pp. 277–286).

Wiedenbeck, S., Waters, J., Birget, J.-C., Brodskiy, A., & Memon, N. (2005a). Authentication using graphical passwords: Effects of tolerance and image choice. In Proceedings of the 2005 symposium on usable privacy and security (pp. 1–12).

Wiedenbeck, S., Waters, J., Birget, J.-C., Brodskiy, A., & Memon, N. (2005b). Passpoints: Design and longitudinal evaluation of a graphical password system. Inter-national journal of human-computer studies, 63(1), 102–127.

Yampolskiy, R. V. (2007). User authentication via behavior based passwords. In Systems, applications and technology conference, 2007. lisat 2007. ieee long island (pp. 1–8).

Zhao, H., & Li, X. (2007). S3pas: A scalable shoulder-surfing resistant textual-graphical password authentication scheme. In Advanced information networking and applications workshops, 2007, ainaw'07. 21st international conference on (Vol. 2, pp. 467–472).

APPENDIX A

Research Papers

1. Ranak, M. N., Azad, S., Nor, N. N. H. B. M., & Zamli, K. Z. (2017). Press touch code: A finger press based screen size independent authentication scheme for smart devices. PloS one, 12(10), e0186940.
2. Azad, S., Rahman, M., Ranak, M. N., Ruhee, B. K., Nisa, N. N., Kabir, N., ... & Zain, J. M. (2017). VAP code: A secure graphical password for smart devices. Computers & Electrical Engineering, 59, 99-109.
3. Ranak, M. N., Azad, S., Mohammad, S. A. B., Zamli, K. Z., & Rahman, M. M. (2017). 5th International Conference on Software Engineering & Computer Systems, 2017.

Awards

1. Gold in IENA-2018, GERMANY, with project ”(VAP) code : a smart and secure authentication sceme.”
2. Gold in ITEX-2017, MALAYSIA, with project ”(VAP) code : a smart and secure authentication sceme.”
3. Gold in ICE - CLnno , 2016 , ump , with project ”A Secure Shoulder Surfing Registrant Authentication Scheme.”

APPENDIX B

Sample generated press data

0.000686656,0.004180972,0.010986496,0.048447393,0.068284124,0.10215915,
0.1132372,0.14366369,0.16229495,0.17642482,0.20466927,0.21576257,0.2409247,
0.25516137,0.26413366,0.28926528,0.30037385,0.33411154,0.34309912,0.38202488,
0.4138857,0.45491722,0.46218053,0.49338523,0.50952923,0.51841,0.5308461,
0.5342794,0.537087,0.5371023,0.53290606,0.50238806,0.48830396,0.4350805,
0.40277714,0.35988402,0.3303273,0.32289615,0.31218433,0.30948347,0.30785078,
0.30678263,0.30714884,0.31313038,0.34335852,0.3803769,0.38551918,0.39632258,
0.41345847,0.41744107,0.42253757,0.42325476,0.42279696,0.42078277,0.382681,
0.37524986,0.34354162,0.32343024,0.31259632,0.2964828,0.2806592,0.27728695,
0.27493706,0.272343,0.2719005,0.27278554,0.27547112,0.3216907,0.33568323,
0.38307774,0.41570154,0.42307165,0.45188066,0.46305028,0.47258717,0.47489128,
0.47632563,0.47609675,0.4704509,0.43920043,0.42827496,0.38069734,0.34857708,
0.3083238,0.30220494,0.27397573,0.2628977,0.25392538,0.23988709,0.22949569,
0.22771038,0.22626078,0.2262913,0.22691691,0.24022278,0.27476922,0.31903562,
0.3528954,0.3990997,0.40531015,0.41976044,0.43608758,0.441413,0.4470741,
0.447776,0.4470741,0.4447242,0.40006104,0.38892195,0.3561303,0.31631953,
0.28894484,0.2701457,0.26665142,0.26399633,0.26141757,0.2610361,0.26182956,
0.2640879,0.30432594,0.3152819,0.36266118,0.3937438,0.39987794,0.42552835,
0.43163195,0.43814754,0.4394293,0.43961242,0.4383917,0.43439382,0.39108872,
0.3573663,0.31496146,0.307805,0.28218508,0.27122912,0.2589456,0.25241473,
0.24919508,0.24858473,0.24856947,0.24936293,0.25639734,0.27597466,0.29018083,
0.320943,0.3510033,0.36229494,0.36951247,0.37798125,0.38059053,0.38274205,
0.38287938,0.38252842,0.37781337,0.36668956,0.32814527,0.29739833,0.27809566,
0.26717022,0.25635156,0.24290837,0.23776607,0.2322118,0.23108263,0.23093003,
0.23218128,0.26796368,0.27521172,0.30844587,0.35091174,0.35696957,
0.38191807,0.38913557,0.39816892,0.4004425,0.40196842,0.40195316,0.40109864,
0.38764018,0.3562066,0.3300679,0.32118714,0.29980928,0.2872816,0.28033876,
0.27855346,0.27747005,0.27785152,0.28564888,0.3185626,0.32971695,0.37813383,
0.41022354,0.43758297,0.446479,0.46253148,0.46588847,0.46915388,0.46930647,
0.46878767,0.45593956,0.4206302,0.38181123,0.3481956,0.30565345,0.29951933,

```
0.26091403,0.29423973,0.3084001,0.35211718,0.3838102,0.40003052,0.4087129,
0.41661707,0.41849393,0.41939422,0.4187991,0.41722745,0.3795529,0.37068743,
0.3312276,0.3004349,0.28722057,0.27627984,0.26752117,0.25691617,0.2538796,
0.25148395,0.25143817,0.25520715,0.28644237,0.3004349,0.35387197,0.3849546,
0.41211566,0.41937897,0.42917526,0.43126574,0.43266958,0.43244067,0.43118945,
0.3966125,0.38794538,0.34619668,0.3143206,0.27554742,0.27032882,0.2399939,
0.22000457,0.21110857,0.1858091,0.17689784,0.1537499,0.14502174,0.129045550
```