Secure Multilevel Authentication Schemes to Protect Session Passwords

Ph.D Thesis

By

Syed Shabih Ul Hasan
124-FBAS/PHDCS/F15

Supervisor

Dr. Anwar Ghani
Lecturer

Department of Computer Science & Software Engineering
Faculty of Computing
International Islamic University, Islamabad
2022

Authentication (Computer science)

Computer security

Password management

Access control

Cryptography

Multilevel authentication

A dissertation submitted to the
Department of Computer Science & Software Engineering,
International Islamic University, Islamabad
as a partial fulfillment of the requirements
for the award of the degree of
Doctor of Philosophy in Computer Science

Plagiarism Undertaking

I take full responsibility for the research work conducted during the PhD Thesis titled "Secure Multilevel Authentication Schemes to Protect Session Passwords". I solemnly declare that the research work presented in the thesis is done solely by me with no significant help from any other person; however, small help wherever taken is duly acknowledged. I have also written the complete thesis by myself. Moreover, I have not presented this thesis (or substantially similar research work) or any part of the thesis previously to any other degree awarding institution within Pakistan or abroad.

I understand that the management of International Islamic University Islamabad has a zero-tolerance policy toward plagiarism. Therefore, I as an author of the above-mentioned thesis, solemnly declare that no portion of my thesis has been plagiarized and any material used in the thesis from other sources is properly referenced. Moreover, the thesis does not contain any literal citing of more than 70 words (total) even by giving a reference unless I have the written permission of the publisher to do so. Furthermore, the work presented in the thesis is my own original work and I have positively cited the related work of the other researchers by clearly differentiating my work from their relevant work.

I further understand that if I am found guilty of any form of plagiarism in my thesis work even after my graduation, the University reserves the right to revoke my PhD degree. Moreover, the University will also have the right to publish my name on its website which keeps a record of the students who plagiarized in their thesis work.

Syed Shabih Ul Hasan: 

Date: 30 - Nov - 2022

INTERNATIONAL ISLAMIC UNIVERSITY ISLAMABAD
FACULTY OF COMPUTING
DEPARTMENT OF COMPUTER SCIENCE & SOFTWARE ENGINEERING

Date: 26-10-2022

Final Approval

It is certified that we have read this thesis, entitled "Secure Multilevel Authentication Schemes to Protect Session Password" submitted by **Syed Shabih ul Hassan Registration No. 124-FBAS/PhDCS/F15**. It is our judgment that this thesis is of sufficient standard to warrant its acceptance by the International Islamic University Islamabad for the award of the degree of PhD in Computer Science.

Committee

External Examiner:
Dr. Basit Raza,
Associate Professor,
COMSATS-Islamabad

External Examiner:
Dr. Arif ur Rehman,
Associate Professor,
Bahria University-Islamabad

Internal Examiner:
Dr. Imran Khan,
Assistant Professor
Department of Computer Science & Software Engineering
FoC, IIUI

Supervisor:
Dr. Anwar Ghani,
Lecturer
Department of Computer Science & Software Engineering
FoC, IIUI

Declaration

I hereby declare that this thesis, neither as a whole nor as a part thereof has been copied out from any source. It is further declared that no portion of the work presented in this report has been submitted in support of any application for any other degree or qualification of this or any other university or institute of learning.

Syed Shabih Ul Hasan

Dedication

I dedicate my dissertation work to my family and many friends. A special feeling of gratitude to my loving parents, whose words of encouragement and push for tenacity ring in my ears. My wife and my daughter have never left my side and are very special.

I also dedicate this dissertation to my many friends who have supported me throughout the process.

Syed Shabih Ul Hasan

Acknowledgments

This thesis would not have been possible without the inspiration and support of several wonderful individuals — my thanks and appreciation to all of them for being part of this journey and making this thesis possible. Foremost, I would like to express my sincere gratitude to my supervisor, *Dr. Anwar Ghani*, for giving me guidance and counsel and having faith and confidence in me. His guidance helped me in all the time of research and writing of this thesis. I could not have imagined having a better advisor and mentor for my Ph.D. study. He read and correct my early attempts at writings.

Besides my supervisor, I would like to thank the rest of my thesis committee: Dr. Qamar Abbas, Dr. Nadeem, and Dr. Imran Khan, for their insightful comments and encouragement, but also for the hard question which unscented me to widen my research from various perspectives.

I sincerely acknowledge the contribution of different collaborators: Dr. Muhammad Billal, Hankuk University of Foreign Studies, South Korea, Dr. Alireza Jolfaei, Macquarie University, Australia, Dr. Ikram Ud Din, University of Haripur and Dr. Ali Daud, College of Computer Science and Engineering, University of Jeddah. I am extremely grateful to these stalwart personalities who guided me.

This achievement would not have been possible without the pure love and support of my family and friends. They back me in every hurdle I faced during this travel. I am forever indebted to them for giving me the opportunities and experiences that have made me who I am.

List of Publications From Thesis

1. **Syed Shabih Ul Hasan**, Anwar Ghani, Muhammad Bilal and ALireza Jolfaei "Multi-Factor Pattern Implicit Authentication" IEEE Consumer Electronics Magazine, IEEE, 2021, 11 (1): 26-32. *(Impact factor 3.789)*

2. **Syed Shabih Ul Hasan**, Anwar Ghani, Ikram Ud Din, Ahmad Almogren and Ayman Altameem "IoT Devices Authentication Using Artificial Neural Networks", Accepted for publication in CMC-Computers, Materials & Continua, Tech Science Press, 2021, 70(2): 3701-3716. (Impact factor 3.772)

Articles in Progress

1. **Syed Shabih Ul Hasan**, Anwar Ghani, Ali Daud "Secure Authentication Mechanisms: A Review". SN Computer Science, Springer, 2021.

2. **Syed Shabih Ul Hasan**, Anwar Ghani "A Hybrid Model for Mobile Authentication Using CNN". IEEE Internet Computing, IEEE, 2022.

Acronyms

OP-Grid Operation Grid
PPA Processed Password Authentication
IBAM Machine Learning Instruction Based Handwritten Authentication
MPAS Mobile Password Authentication Schemes
FAR False Acceptance Rate
FRR False Rejection Rate
SVM Support Vector Machine
ANN Artificial Neural Network
RBF Radial Basis Function Kernel
DTW Dynamic Time Wrapping
KNN K-Nearest Neighbour
CNN Convolutional Neural Network
EER Equal Error Rate
AUC Area Under Curve
ROC Receiver Operating Characteristic
RNN Recurrent Neural Network
LSTM Long Short Term Memory
HOG Histogram of Directed Gradients
SSL Secure Socket Layer
ACC Accuracy
ANFIS Adaptive Neuro Fuzzy Inference system
LMNN Large margin nearest neighbor
RSF Response Satisfaction Factor
PIN Personal Identification Number
GPS Global Positioning System
Wi-Fi Wireless Fidelity
PDA Personal Digital Assistant
R-code Registration Code
P-code Process Code

Abstract

Smartphone functionality includes social networking, online shopping, mobile gaming, private/ group communication, and other functions that are widely utilized and pervasive in nature. When using these services, users must provide private information, which is subsequently saved on the device, such as account credentials, credit card information, etc. If this information is lost, a user's privacy may be compromised, and they may suffer financial loss. Therefore, protecting such devices from illegal access becomes essential. Regardless of the importance of security and privacy, smartphones are still secured by conventional authentication methods like PINs, passwords, and pattern locks, which are well-known for their flaws in the security world. Smartphone authentication has recently incorporated physical biometrics like facial, fingerprint, and iris recognition; yet, these techniques still have usability and security challenges. Therefore, it is necessary to develop innovative, precise, and user-friendly authentication systems. In this context, methods for behavior-based authentication have recently sparked a lot of attention in both the professional and academic worlds. Behavior-based authentication has shown to be fairly effective at authenticating users by using an individual's unique features for identification. The majority of smartphone users prefer convenience over security and find authentication processes to be more unpleasant than other technical issues like poor coverage, excessive power use, etc. This research addresses the shortcomings of the current authentication techniques with regard to security and usability and suggests behavioral biometric-based authentication mechanisms as a solution. The proposed system is a combination of both explicit and implicit authentication. A user has to draw patterns or draw the PIN code numbers on the screen of the smartphone which is an explicit authentication technique, then with the use of the implicit technique, the drawn pattern or PIN codes are used for behavior recognition with the features of velocity, speed, time and pressure. This multi-factor behavioral authentication method has two phases of security. First will judge the correctness of the input pattern or PIN codes and then will judge the legitimacy of the gesture by the user's login behavioral features. These two phases make two lines of defense by which the authentication method is difficult to break or steal. The obtained results show the value of FAR 4.36 and FRR 5.03 and an AUC of 95%. Furthermore, a comparative analysis of the proposed methods with the existing authentication techniques based on accuracy, performance, usability, and different attacks. The comparative analysis also shows that the proposed technique perform better than their competitors.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Interests or aims by which people look around to change or exploit the environment are referred to as technology. By the time technology is growing advanced and now become a requisite part of life. In the history of mankind, the smartphone symbolized one of the most spacious and advantageous technological ideas. The mobile phone was first revealed by the Motorola Company by Dr. Martin Cooper in 1973 to make and receive calls [1]. The smartphone is a device that combines the functionality of both a cellular phone and a handheld computer. A headway to technological advancement, smartphones are becoming an essential part of our daily routines. It took different pieces of technology and put them together into one that began with various fitness apps to track the distance traveled, time availability, calculator, calendar, music, videos, speed, and calories burned using GPS and in leisure time broaden up to managing resources on a single click at the personal device. With access to the internet, every single work of art of human knowledge that existed is now in our pocket. Moreover, it provides functionality such as social networking, online shopping, mobile gaming, and private/group communication that are fast, attractive, and powerful. It provides storage for important data for example personal details, information, and files. In pleasure the workplace, smartphones inflate our potentiality and assist us in sorting our problems in a convenient manner. All the functionalities mentioned made the smartphone almost unmatched [2].

Any action to intercept the venomous use or coincidental harm to the user's private data is referred as security. It's about minimizing the risk. By providing knowledge to the user about how to run the apps under secure mode we can implement the security. Along with the smartphones traditional use (calling and texting) they also perform multiple activities, such as online banking and shopping, social networking, taking pictures, and e-mailing which are security sensitive. By pro-

viding user's desired services smartphones enhanced the standard of living meanwhile they cause security and privacy threats to the data that is stored by user. The data contains contacts, mailing addresses, passwords, name, age, essential banking details, etc. This indicates the seriousness of mobile security, as phone is appraised to be a valued target for hackers. The retrieving of the corporate resources from user's personal device is increasing the vulnerability of data being exploited by strangers. Preventing the unauthorized access to the sensitive information on smartphone the first line of defense is user authentication. Authentication is the process of recognizing users that request access to a system, network, or device. Smartphones are small, portable, beneficial and efficient that's why we carry them along with us all the time, in this manner the physical security of smartphones is also a dominant consideration. The most prevailing threat to smartphones is the stealing or lost, because it carries the sensitive information regarding user and its hardware can also be re-sold. In the modern world, smartphones are involved in every area of people's lives. People can use cellphones, for instance, for activities like learning, making new acquaintances, and shopping. The smartphone has boosted up life and provided convenience, but on the other hand, it has also led to an increase in dependence on or even addiction to cellphones among people. [3]

If the PIN/pattern is compromised, it can be renewed. Biometrics can't be renewed once they've been compromised, therefore they're useless and gone permanently. It is possible to reassemble a fingerprint [4]. Jan Kreisler, a biometric hacker, was able to replicate the fingerprint of Germany's defence minister and gain access to her iPhone [5]. Fake positives are silicone finger impressions used to gain access to sensitive data. If a biometric system is slightly altered, it can cause scanning complications. It is impossible to change or alter fingerprints once they have been stolen.

There are many treats on the security of smartphones in various manners [6]. For example, one can make changes to a user's phone bill, send unsolicited messages to a user's contact list, or give an attacker control over a user's device, collecting or using the user's private data that includes phone call history, text messages, user location, browser history, contact list, email, and private photos without the knowledge of the user. One can send links through different mediums like email, messages, Facebook, and Twitter that trick the user to provide sensitive information. Taking advantage of the flaws in the operating system or poor Wi-Fi one can also get access to users' sensitive information. This stolen information could be used for identity theft or financial fraud. The focus is on the techniques and methods of authentication to strengthen smartphone security.

1.1 Motivation

Numerous mobile phone programs, also known as smartphone apps, have infiltrated every aspect of our life due to the exponential rise of mobile communication technology. Smartphone apps are described as "end-user software program's that are created for a mobile operating system and which extend the phone's capabilities by enabling users to do certain tasks".Mobile users can access such apps anytime, anyplace as a hub for a range of content and services. Consumers may use their cellphones to handle a variety of daily tasks thanks to mobile phone apps. An app can be used by a customer to make purchases, and pay bills etc. [7]. Any authentication method's main goal is to prevent anyone from using the devices without authorization.

Security is at its best when it satisfies the sole aim of securing computing atmospheres with the least amount of endangering usability. User eased security, has been the main motive of all of the researchers and scholars in the corresponding field. As the mobile showcasing measurements accumulation by Danyl, the mobile shipments had surpassed PC shipments in 2011, and the number of portable clients likewise overwhelmed work area clients in 2014, which shut to 2 billion [8]. In any case, bear surfing assaults have represented an extraordinary risk to clients' protection, what's more, privacy as cell phones are getting to be vital in current life. Individuals may sign into web administrations also, applications openly to get to their records with their PDA's, tablets, or open gadgets, similar to bank ATM's. Shoulder-surfing assailants can see how the passwords were entered with the assistance of reflecting glass windows or not to mention screens hanging wherever in open spots. A safe validation framework ought to most likely guard against bear shoulder surfing and should be relevant to all sorts of gadgets. The limitations of usability include issues such as taking more time to log in, passwords being too difficult to recall after a while, and the authentication method is too complicated for users without proper education and practice.

Shoulder attack is one of the most recent weapon utilized by hackers in an association to hack an account [9]. In this type of attack, a bystander is watching the user when he is entering his password or record his finger movements on the keyboard through a camera. This type of attack normally occurred in public places and in organizations. Textual passwords are more vulnerable to shoulder surfing, as user types the same password many times a day with the same keyboard pattern. This makes it necessary that techniques must be developed which can prevent password entry from this attack. Many researchers have provided different solutions against shoulder surfing, using graphical passwords and formula based authentication system. The standard four-digit PIN code or mobile phone pattern lock authentication, are fairly simple to use and largely accepted

by the public. However, the safety of such techniques is debatable. Indeed, it is rather simple for someone to observe the PIN code or pattern being drawn and then steal it. As a result, novel authentication mechanisms such as randomized PIN codes and a random pattern for each login attempt provide a higher level of security. Even if someone witnesses the PIN code being entered or the pattern being drawn, they will not be able to duplicate it, this will help in avoiding the shoulder surfing attack. [10].

If the PIN/pattern is compromised, it can be renewed. Biometrics can't be renewed once they've been compromised, therefore they're useless and gone permanently. It is possible to reassemble a fingerprint [11]. Jan Kreisler, a biometric hacker, was able to replicate the fingerprint of Germany's defense minister and gain access to her iPhone [5]. Fake positives are silicone finger impressions used to gain access to sensitive data. If a biometric system is slightly altered, it can cause scanning complications. It is impossible to change or alter fingerprints once they have been stolen.

In certain situations, biometric recognition is a viable approach to solving some of these limitations and addressing password security problems. The increasing number of smartphones that support unlocking using biometric modalities has driven the push toward biometrics in recent years. The fundamental issue with these biometrics is that they are easy to observe and cannot be modified or canceled once they have been compromised. It is possible to remove fingerprints from smooth surfaces (such as a smartphone screen or coffee cup). However, as high-resolution cameras become more widely available, capturing them from a distance has become a new attack vector. Using only a few high-definition pictures, hackers were able to effectively collect the fingerprints of German Minister of Defense Ursula von der Leyen in 2016 [12].

While physiological biometrics is the most well-known and commonly employed, their behavioral counterparts have recently received a lot of interest. Keystroke dynamics (distinctive typing patterns), touch dynamics (characteristic touchscreen inputs), gait, eye movements, and other behavioral biometrics are examples. One significant advantage is that they are far more difficult to observe because they do not leave physical marks that may be retrieved or photographed. Furthermore, behavioral data can frequently be collected constantly during system operation (e.g., mouse movements or keyboard dynamics) without needing the user to take any explicit actions. The purpose of this thesis is to provide a thorough examination of the security offered by behavioral biometrics. As a result, we concentrate on behavioral biometrics design, evaluation, and security analysis. For this thesis, we have identified three main components:

1. biometrics-based authentication system

2. validation methodologies
3. security analysis against effective threats

1.2 Scope of the Research

The design and security evaluation of behavioral biometrics in the context of authentication is the main emphasis of this thesis. This thesis doesn't include authentication technologies like fingerprint scanning, which are routinely used for a one-time authentication. The justification is that continuous biometric sensing (for example, continuously asking the user to scan their fingerprint) is impractical. Biometric recognition is frequently cited as a benefit that improves usability. While we collect user feedback throughout the several experiments that make up this thesis, this study does not rely on rigorous usability-focused user research. The proposed frameworks are capable of meeting higher security needs and providing ongoing protection to ensure the current user's legitimacy.

1.3 Challenges

Most users accounts are protected which are related to their life like getting information, getting entertained, doing business, emails, uploading and sharing their pictures to albums, clouds and searching. They can access them by logging into it and while doing it in public can expose their all secretive password to suspicious parties without knowing. There would be many in a crowd which will have a malicious intent and can have an eye on your password entry from the keyboard or screen and the relatively sharp memory to remember your password which in today's world is known as Shoulder surfing. If you rather have a difficult password, then there is another gadget or electronic device which will help these malicious intent people to get your password and this would be the omnipresent video cameras recording it all. If the attacker gets to know the collection of alphabets numeric and symbols that comprises of your password from your key strokes of the keyboard or touches on the screen, then there is not stopping. The attacker has access to all what only you can legally would.

The problems which we would like to discourse in this study are as follows.

- Shoulder surfing attacks in public places or in office/home is appeared as a problem when someone is close by peeking [13]

- Secure authentication is possible with the use of augmented devices [14] but these devices are expensive and not in reach of every computer user and why a user should carry an extra device for the purpose of authentication. [15].
- Authentication scheme should be user friendly when it combines the graphical pad system with something user process authentication factor [16, 17].

1.4 Research Questions

The scope of the work defines the following specific research questions

1. How the shoulder surfing attack can be avoided using simple and reliable graphical authentication techniques?
2. How successful is this biometric technique for user authentication?
3. What is the level of security when graphical authentication is used in the context of different attack models without the use of extra hardware device?

1.5 Aims and Objectives

The objective of the proposed system is to enhance the usability features of the authentication system by developing a graphical pad and an on screen keyboard that fulfils most of the usability requirements. The main usability characteristics of the proposed systems are highlighted as follows:

- Being one of the most common attack, the authentication system should also be robust against the shoulder surfing attack.
- The goal of this thesis is to introduce a combination of graphical authentication schemes with behavioural biometric features that can accurately differentiate people, and provide resistant to possible attacks.
- There should be nothing to carry, which means that a user should not rely on auxiliary devices (e.g., tokens) to perform the authentication task.

1.6 Problem Statement

Traditional approach such as pin and pattern locks are being used for the authentication that are vulnerable to security threats [18]. Because of similar layout of keyboard and unlock pattern shape, the traditional approaches suffer from "Less password space", problem [19]. Some of the threats do not require the attacker to have extra technical knowledge or device i.e., shoulder surfing, smudge attacks [20].

Gadgets are used in traditional authentication systems to identify users, however these gadgets can be misplaced, stolen, or left behind [21]. Since it does not rely on items but rather the individuals' physical traits, biometric authentication has been used as an alternate strategy for user authentication. Due in part to human unreliability, current biometric devices cannot guarantee accuracy of 100% [22].

In other cases, physiological biometric features (Face, fingerprint, hand geometry, palm print, iris, voice, signature) were also utilized. With regard to one of them; the usage of fingerprints, there is a concern that some individuals feel infringes their right to privacy. Furthermore, researchers have shown that gelatin fingers made to look real can be used to dupe biometric fingerprint scanners [23]. Additionally, the user must maintain their finger on the scanner that is built into the gadget in order to validate their fingerprints. Further, due to the position that users must adopt in front of a sensor, alternative physiological biometric technologies, such as facial recognition, are not thought to be practical for many users.

1.7 Research Contributions

This dissertation covers the challenges towards secure and reliable authentication using machine learning techniques. We proposed three frameworks for effective authentication performance. The design, implementation, and technical details of innovative systems for user authentication on smartphones are presented in this dissertation. The following is a list of this thesis's research contributions.

- To provide a defence mechanism against shoulder surfing and smudge attacks, this thesis proposes a OP-Grid approach which is an implicit graphical authentication scheme. An authentic user is identified not only by the pattern they generate but also by how they do it utilizing finger velocity and stroke time data.

- This study offers a Process-based Pattern Authentication (PPA) solution for Internet of Things (IoT) devices that eliminate the need for a server to keep a record of the login user's static pattern. The server saves the information users supply during registration, such as the Registration code and the symbol, but the Process code, i.e., the actual password, changes with each login attempt. Users can create a pattern based on the Process code and Registration code in the PPA pattern and authenticate themselves using their touch dynamic behaviors.
- This study introduces Instruction Based Handwritten Authentication (IBAM), which uses something you process as an authentication factor. Every time a user tries to log in, the server sends them two numbers and a mathematical operator. The PIN codes are requested to be drawn instead of inputting them on a touch pad of mobile devices. IBAM provides enhanced security by combining behavioral biometrics with a new processed password at each login attempt as an extra authentication factor apart from the PIN's concealment.

1.8 Thesis Organization

The thesis' main chapters are based on research articles written throughout the PhD program.

Chapter 2 explains the importance of a secure authentication mechanism and how machine learning algorithms are useful in this regard.

Chapter 3 reviews the literature and provides the background relevant to the context of the thesis. The associated techniques and literature are classified into seven different categories. This section helps us to identify research gaps, challenges, and directions for strong authentication scheme.

Chapter 4 introduces the in depth analysis of three proposed proposed solution. The methods proposed in this thesis make the login more secure and safe from shoulder surfer and smudge attacks.

Chapter 5 discussed the first proposed methodology. The proposed technique takes the fifth level of authentication factor and creates a graphical authentication system called Operational Grid (OpGrid) to overcome the pattern lock system's shortcomings.

Chapter 6 discussed the third proposed methodology. The proposed multi-factor behavior authentication technique i.e., Processed Pattern Authentication (PPA) uses the "something you process" factor, in which the user's drawn pattern is examined, i.e., whether it is valid or not, and the accuracy of the drawn pattern is later determined by using the user's login behavioral attributes.

Chapter 7 discussed the third proposed methodology. and proposes a Instruction Base authentication (IBAM) system that allows users to login with a unique PIN each time. A set of effective features that record behavioural information while typing PIN codes on touch displays makes this scheme more secure.

Chapter 8 concludes the thesis with a summary of the main findings and a discussion of future research directions.

Chapter 2

Background

There are many threats to the security of smartphones in different manners. For example, one can make changes to a user's phone bill, send unsolicited messages to a user's contact list, or give an attacker control over a user's device, collecting or using the user's private data that includes phone call history, text messages, user location, browser history, contact list, email, and private photos without the knowledge of the user. One can send links through different mediums like email, text messages, Facebook, and Twitter that trick the user to provide sensitive information. Taking advantage of the flaws in the operating system or poor WiFi one can also get access to users' sensitive information. This stolen information could be used for identity theft or financial fraud. The focus is on the techniques and methods of authentication to strengthen smartphone security.

Due to its persistence and individuality, human biological data can be utilized for access control, identification and authentication. Biometric authentication is the utilization of biological data for user authentication. It has two major types, i.e. physical and behavioural biometrics. Behavioural biometrics is based on behaviours characteristics that include gait, keystroke, voice, signatures and physical biometrics depends on the physical properties i.e. hand geometry, retina scans, iris or fingerprints. Because its alphanumeric counterparts can be stolen, forgotten, and shared, biometrics has the potential to fully replace knowledge-based solutions. Biometric authentication has long been researched. Fingerprint sensors in laptops and mobile phones are examples of large-scale commercial implementations. These installations, on the other hand, are based on physical biometrics, which effectively demands intentional user activity, resulting in user annoyance [24] and providing a "one-shot" authentication.

Behavioural biometrics have been used in the majority of studies on transparent, implicit, and con-

tinuous authentication in smartphone security and access management. When compared to physiological features, behavioural biometrics have some advantages. When compared to physiological features, behavioural biometrics have some advantages. One of the most significant advantages is that behavioural patterns can be collected invisibly, or even without the knowledge of the user. Furthermore, data collecting does not involve the use of any special hardware platform. However, the majority of the behaviours are not distinct enough to serve precise user identity, but they have shown promise in terms of user verification [25].

On the basis of data gathering method, recent literature divides human activities into five categories [26].

- **Biometrics based on authorship:** Verification and identification of users based on the way they write or draw on a paper.
- **Direct Human Computer Interaction:** In their everyday interactions with computers and new generation gadgets, different users adopt different techniques, styles, and apply their abilities and expertise in diverse ways.
- **In-Direct Human Computer Interaction:** Metrics acquired by indirectly observing user HCI activities through low-level computer programme actions. Audit logs [27] and registry access [28], for example, are used to identify people.
- **Kinetics:** It is a human's ability to use his or her muscles [28]. These movements, which rely on the appropriate functioning of the brain, joints, bones, and neurological system, consequently reflect the quality of those systems' functioning, allowing verification.
- **Behavioral Biometrics:** It analyzes human behaviours that aren't immediately related to body part measurements or intrinsic, unique, and long-lasting muscle activities, such as how a person types or walk.

2.1 Biometric Authentication

For every system that is based on biometric recognition, it is obligatory to recognize a person by its features (physical, and behavioural) in accordance with the relevant questions submitted by that person. An imaginary biometric must have "zero" false acceptance and false rejection values and must assure other attributes, such as completeness, singularity, stability, and rightness and must be strong against potential attacks. A block diagram figure 2.1 of the four-dimensional biometric

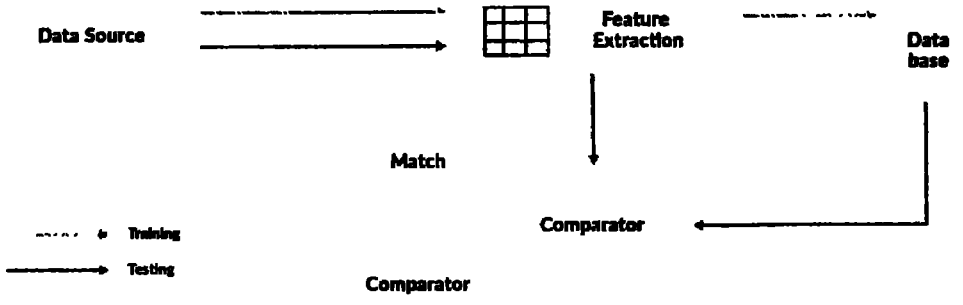

Figure 2.1: Dimensions of Biometric authentication system

system, is described below:

2.1.1 Data Source

The block is about capturing individual's biometric data including the hardware as well as the software. Besides, it can add an auxiliary "Quality Checker" item, to confirm the quality of data.

2.1.2 Feature Extraction

The block is concerned with the removal of preferential attributes from a biometric sample already collected to obtain the information of the relevant user in the database.

2.1.3 Database

In this block the biometric template produced from the data. This template data is use to validate between the authorized and unauthorized user.

2.1.4 Comparator

The block compares the declared or question pattern with the original patterns (s) already saved, and determines the acceptance/rejection. To verify, it will match individually and to identify, it will match the input. The identification of the user is based on the best attained score after querying all the saved patterns of all the classes (1:N).

2.2 Identification vs. Biometric Verification

The term "authentication" or "verification" refers to the process of confirming one's identity. When a user asserts his/her identity (for example, by putting a card into an ATM machine or inserting a card to get access to secure facilities and then typing a password or PIN), the system executes certain computations to verify the user's assertion. A 1:1 match take place when an assertion is compared to a template that has been saved earlier. Identification is different from verification in the way that the unknown query template is provided by a known user, and the system's job is to match it to a known user's template. This is referred to as 1:N matching. Open-set and closed-set identifications are the two types of identification. If the template exists in the classifiers database for the users being verified earlier, this identification is known as closed set; otherwise, it is open set. The problem of authentication is the major subject of this thesis.

2.3 Biometric Traits Choices

Apart from their recognition performance, the choice of biometric modalities is influenced by a number of parameters. According to the literature [29] there are seven parameters to consider when determining the suitability of these features, which are outlined below:

1. Universality: That biometric modality is required for every user. This parameter is used to calculate the FTER (Failure to Enroll Rate) of a biometric system.
2. Uniqueness: In a group of people, the provided modality should be sufficiently varied.
3. Consistency: Over a period of time, the provided modality must be consistent.
4. Measurability: The ability to capture and process biometric data using the best technology without causing the user any inconvenience.
5. Performance: Aside from recognition accuracy, the biometric system's throughput must be able to cope with the application's limits.
6. Acceptability: It reflects how simple and comfortable it is for users to input their traits to the system.
7. Circumvention: It relates to the simplicity with which other participants' modalities can be duplicated, reproduced, or modified in order to gain unauthorized access to the system.

2.4 Smartphone Sensors

There are three kinds of mobile sensors named as motion sensors, position sensors and environmental sensors [30]. Accelerometers, gyroscopes, gravity sensors are the motion sensors which compute the acceleration and force of rotation along axes(x,y and z). Orientation and magnetometer sensors are the position sensors which compute the smartphone's physical position. Environmental sensors (Barometers, thermometers, etc) compute several environmental parameters. Movement and position sensors proclaim to be correct regarding the selection of users and are utilizing broadly for authentication of users in smartphones [31, 32]. Environmental sensors may not be beneficial regarding the "shot-one" authentication, rather it can be beneficial for continuous verification. We have used the position and motion sensors in this study. In the operating system of mobile (Android), ensuring the registration of a sensor via a registerlistener() known as Sensor Delay Modes [30], the collection of data can be done using fixed as well as the customized periods. Four of the fixed intervals namely, `SENSOR_DELAY_FASTEST`, `SENSOR_DELAY_GAME`, `SENSOR_DELAY_UI` and `SENSOR_DELAY_NORMAL` are supported by android. `SENSOR_DELAY_FASTEST` without any delay in throwing samples, `SENSOR_DELAY_GAME`, `SENSOR_DELAY_UI` and `SENSOR_DELAY_NORMAL` with fixed delay of 20,000 μ seconds, 60,000 μ seconds and 200,000 μ seconds respectively. Following is the explanation of the working principle regarding our chosen sensors:

2.4.1 Accelerometer Sensor

It computes the acceleration practiced on this device along with the gravitational force calculated on the axis (X, Y and Z). Android API utilizes the upgraded system that must have three-axis coordinates.

The application of the acceleration used to the mobile device A_m is computed by the use of the forces (including the gravitational force g) applied to the F_m sensor itself utilizing the equation.

$$A_m = -g\sum \frac{Fs}{mass} \tag{2.1}$$

For the removal of the contributed gravitational force regarding the unprocessed accelerometer data, application of High Pass Filter (HPF) was done by us and we acquired the HPF accelerometer readings. The inspiration was to acquire the accurate acceleration that was applied over the device by the user. On the other hand, the application of the Low Pass Filter (LPF) to the unprocessed accelerometer data was done for acquiring the obvious transient forces that act upon the device,

originated by the activity of the user.

2.4.2 Gyroscope Sensor

The sensor computes the smartphone's rotation rate (rad/s) along the three dimensions. The co-ordinate system of this sensor are similar to them that were utilized for acceleration sensor. The result is positive for the rotation (counter-clock-wise). Expressly on a condition that a viewer is watching the device from a good spot (utilizing the three axis) is known to be positive.

2.4.3 Magnetometer Sensor

This sensor computes the force as well as the direction (in some cases) of the magnetic field (μT) along the three dimensions. It doesn't cover the north point, so it is different from the compass. It also computes the magnetic field of the earth in case the device is located in a domain completely free of magnetic involvement.

2.4.4 Touchscreen

It gives the device's operating interface to the user. Devices can be classified into the single touch devices and multi-touch devices. The pen and the finger serve as a contact tool for the touch screen. Specifically, for Android, the library MotionEvent offers a class for tracking the movements of various indicator like fingers, stylus, mouse, trackball, etc. The incident that was caused by the touch effect is stated by an object of this class. The special action code might be contained by this object as the touch location on XY coordinates of the touch screen, details regarding the pressure, size and orientation of the area that was touched. The state of the touch action is represents by action code for example `Action_Down` and `Action_Up` represents the start and end of a touch action. The Android Velocity Tracker class is being utilized for tracking the pointer's movement over the touchscreen. The class formulas, *getX Velocity()* and *getY Velocity()*, are being utilized for acquiring the pointer velocities over the touch screen along the X and Y axis respectively.

2.5 Machine Learning

Machine learning is the study of motivating systems to learn without the need for manual customization by programmers. It is a subfield of AI that deals with the computational theory and pattern recognition [33]. Machine learning has given us self-driving cars, a reasonable, viable Web

design, and a vastly improved understanding of the human genome in the last decade. Machine learning is now so pervasive that you probably use it daily without even being aware of it. The key concepts of machine learning apply to the field of biometrics to distinguish people based on their behaviour. The following are the key categories of machine learning tasks:

- **Supervised learning:** It includes classifiers such as parametric/non-parametric techniques, kernels, neural networks, support vector machines, and many others.
- **Unsupervised learning:** Clustering, recommender systems, deep learning, dimensionality reduction, amongst many other methods are included.
- **Semi-supervised learning:** In artificial intelligence, it includes best practices such as predisposition and difference hypothesis.

2.6 Classification

Classification is a machine learning technique for distinguishing and categorizing things as they are identified. In machine learning terms, classification is classified as supervised learning, in which the training data is labelled such that it may be accurately identified. Clustering, on the other hand, is an unsupervised learning technique in which the training data is unlabeled and grouping is done using a similarities or dissimilarities metric. Classification is the process of learning about records using training data to identify data points and determine which category they belong to. A classifier is a machine learning method that solves a statistical classification problem. Based on the features and observations or occurrences, the input data is translated to a category. Some features in the dataset are frequently redundant or unnecessary to the classification phase. As a result, after pre-processing the data, they can be filtered out or eliminated without losing information during classification. This is known as an attribute or feature selection, and it involves selecting a subset of the feature set for the classification model. Machine learning algorithms are divided into supervised, unsupervised, and semi-supervised learning approaches based on their ability to generate predictions. Table 2.1 shows different algorithms of machine learning for supervised and unsupervised classification.

The classifications used in this thesis are briefly explained below

Table 2.1: Classification Algorithms

Supervised Learning	UnSupervised Learning
Linear/Polynomial Regression	Singular Value Decomposition
Naive Bayes	Principal Component Analysis
Neural Networks	Measures device rotation through three axes (x,y,z) with roll, pitch, and yaw movements of the smartphone
k-Nearest Neighbour	Hierarchical clustering
Random Forest	Generative Adversarial Networks
Logistic Regression	Expectation-maximization algorithm (EM)
Decision Trees	Hidden Markov models
Support Vector Machines	k means clustering

2.6.1 Support Vector Machines

One of the supervised learning models for pattern identification is the support vector machine (SVM). The idea of linear SVM was first put forth in 1963, while non-linear classification was added in 1992. If sample data fall into one of two classifications, a support vector machine creates a classifier for it. Samples on the margin are referred to as support vectors, and an SVM trains the separation plane with the largest margin. SVMs are among the most effective recognition techniques.

The data of the user executing the pattern for getting authenticated on the smartphone, as captured by the touch sensors, would be stored as a training sample when a user successfully signed in based on the input of his or her pattern; otherwise, the pattern would be discarded. The pattern's authentication could be considered a categorization issue. Illegal users will receive the label 0, while genuine users will receive the label 1. The SVM classifier was trained with the features gathered from various users; the data gathered served as training data and were identified as legitimate users (1). After training, the algorithm evaluates whether a valid user or another user attempted to log in.

2.6.2 Artificial Neural Network

An artificial neural network (ANN) is a collection of interconnected neurons used as a computation model for data management. It is a flexible framework that may alter its course of action in response to the input and yield succession that enters the system. In ANN learning procedures, the calculation of the feed-forward back spread is typical.

All of the neurons in the layers of the neural network's forward pass are propagated to measure the output after the addition of input. The final step involves determining each output neuron's error. In the backward pass, the neurons' hidden weights are altered. Neurons receive measurements and feedback on their hidden layer faults. In this study, the net inputs are identified by locating convolution of inputs with their associated weights. Applying the net output activation function defines the outputs. The logistic function of activation values (zero and one) is used to categorise the succession among them.

2.7 Convolutional Neural Network

Convolutional Neural Networks are among the most widely used deep neural networks. CNNs were developed in order to utilize less data than a conventional artificial neural network (ANN). Three ideas—sparse interaction, parameter sharing, and equivariant representation—are used to decrease the data parameters A CNN's scalability and training time complexity are both improved by reducing the connections between layers. The key benefit of a CNN is that it is widely used in DL training methodologies. Additionally, it enables high-performance automatic feature learning from raw data. The enhancement of image recognition is the primary focus of CNN development. Due to the widespread use of CNNs and the use of several public image sources, successful and efficient models for picture classification and recognition have been developed.

2.8 Summary

The chapter contains the essential background for understanding the problem and the suggested solutions. In the beginning we gave an introduction of biometrics, their various types, and our motive to choose the behavioral biometrics for the solution of the problem. There is complete explanation regarding the system (biometric recognition). We explain the essentials aspects regarding the selection of the biometric modality. We have explained completely about the registration of movements by the user and the movements by the fingers (touch-based factors) utilizing the built-in sensors (3-dimensional) and touchscreen of the smartphone.

Chapter 3

Literature Review

With the emergence of internet of things, mobile password authentication schemes (MPAS) has become much more important in the domain of cyber security. Mobiles and tablets are generally utilized to perform security basic and protection touchy exercises, such as versatile saving money, portable medicinal services, versatile shopping, and so forth. Smart phones will soon be able to support applications across a broad range of domains, including home care, social networks, healthcare, environmental monitoring, protection, and e-commerce, thanks to 5G technology, which offers continuous and secure connectivity [34]. With the advancement in technology the attacking schemes and adversary options have also been widened for hacking, cracking or guessing of a password to gain illegal access into someone else account. There have been many techniques introduced to tackle attacks like shoulder surfing, dictionary attack, brute force etc. Patrick, Long, and Flinn [35] distinguish three security regions for which human factor issues are essential: authentication (passwords), security activities(interruption detection) what's more, creating secure frameworks (building up the security). MPAS is the mechanism of verifying whether or not someone or something is who or what he/she claims to be. While being the first line for the protection of security, the management of user's access authentication requires to be strong, that precisely recognizes all types of camouflage behaviors and comprehend the detection of illegal or venomous objects [36].

Security is at its best when it satisfies the sole aim of securing computing atmospheres with the least amount of endangering the usability. User easement for security, has been the main motive of all of the researchers and scholars pertaining to the corresponding fields. User easement in the field of security bonds all of the aspects related to human beings and intellectual sciences. Passwords

were proved and meant to be the most used security along with strength of bearing any type of attacks by the adversary. Security is the door through which the user will just pass and then do all of the jobs after entering into his authenticated account. A man uses the least amount of time on unlocking the door while entering the office and does whole lot of work inside the office then on the door. So it is to be noticed that this door unlocking process which we call it as the security should be most easy part of the job and so the ease of use should be one the main aspects which should be kept in mind to the issues related to security [37]. While giving solutions and making the system for securing assets there should be a feedback and review for the users using this system so as to make it more powerful and knowing the leakages and suggestions. This process of evolving should be done in the manner that relevant users must be capable of knowing these improvements. The MPAS should be unpredictable so to reduce the risk of exploitation by different authentication attacks [38].

According to mobile market statistics, mobile industry and shipments had overwhelm personal computers industry in 2011, and number of smartphone users also outstrip the desktop computer users at 2014 [39]. People are use to access their web accounts through mobile devices. Normally PIN code or pattern lock is use to unlock the cell phones. Passwords/PIN/pattern lock, even if they are complex and secure, are being exposed to risky environments. People use easy and simple passwords/pattern locks because its easy to recall them. Mobile device security is crucial, and it must be adequate to protect the user and his or her confidential and sensitive data [40]. A secure textual password scheme should provide security against different password attacks. Some of the attacks don't need any extra software to steal the password, like shoulder surfing and smudge attack. Shoulder surfing is a big threat when users access their devices in public places [41]. A shoulder surfer can notice/observe that which letters were pressed or what pattern was followed to unlock the device. In less than one minute, a security team at a global firm used a network password cracker to crack about 80% of the credentials of the employees [42].

Regardless of the fact that smartphones are becoming more popular, the number of input techniques are available for users which are deficient in order to communicate with them. Because the availability of MPAS choices are limited, mobile device manufacturers had to be more innovative with how they incorporate MPAS in their devices. Since attackers are continuously refining their attack methods, MPAS must be strengthened and updated over time [43].

The key contributions of this chapter includes

- The chapter organizes the literature with different MPAS i.e. behavioural authentication and

graphical authentication.

- Insights about standard data sets and performance evaluation of password MPAS.
- A comprehensive discussion on challenges to improve the protection of touch screen cell phones has been addressed and a new viewpoint has been identified for potential research directions.
- A guide on how to improve the safety of touchscreen mobile devices and provides a thorough analysis of major projects

3.1 Authentication : Types and Applications

The schemes which are used around the world for the process of authentication can be divided into following categories [44].

3.1.1 Something user's know

The first type also known as knowledge base authentication, is the use of PIN code or passwords and pattern lock system for authentication [45] [46] [47] [48]. Normally users use simple and easy password or pattern for mobile authentication that can be easily shoulder surfed by a bystander.

3.1.2 Something user's are

This is also referred to as behavioral authentication.This type of authentication involves the authentication with biometric [49] [50] or iris systems [51] [52].

3.1.3 Somebody user's know

This authentication factor is based on social relationships where users may seek the help of a trusted party such as a partner or colleague to help with the authentication process if their credentials fail [53] [54].

3.1.4 Something user's have

The third authentication factor is the use of ATM cards, etc [55] [56].

3.1.5 Something's user process

Recognition base authentication to process the result from given variables, process from instructions to calculate the resulting password. This factor is also known as authentication based on the formula, which was first introduced by Ginzberg [57]. This authentication process requires the user to process a formula in his mind to get authentication according to the numbers or images provided by the server.

3.2 Password Attacks

Users should be enlightened and give awareness about keeping their end of the deal by securing their data and not leaving it unprotected even for an instant. This rule applies to the researchers and developers as well keep the system at the top of its security level. For example shoulder surfer is open to attack at the time of registration and login into a system, which makes the system vulnerable. One should know that the attacker knows, what you know and what you propose, and what are the weakest links in your system which cannot be kept hidden for a lot of time from lots of adversaries around the world. Problems with passwords are that strong passwords are hard to remember and easy passwords are easy to remember but are under threats to different attacks [58].

Password attacks that can harm the MPAS are as follows:

3.2.1 Shoulder Attacks

Shoulder surfing is the latest weapon used by the hacker, through direct observations such as looking over someone's shoulder [59] (figure 3.1) or recording his login or other information by using a hidden camera. This type of attack is an effective way to steal the authentication data, i.e. passwords or PINs, as it requires no extra knowledge of any software [60]. Shoulder surfing is mostly pragmatic for spiteful insiders like friends and colleagues [61].

3.2.2 Brute Force Attacks

This attack uses all the combination of passwords to break the authentication system [62]. Almost every password or encryption key can be break down by using a brute force attack. The amount of time it takes to brute force into the system is an advantage for calculating the security level of the system.

Figure 3.1: A shoulder surfing situation

3.2.3 Dictionary Attack

Dictionary attack is faster than brute force attacks, rather than trying all the possibilities, it uses to catch the passwords with the most common words used by the user in the daily life, i.e. the name of favourite actress, mobile numbers, etc [63].

These passwords can easily be judged by dictionary attacks. This type of attack is limited to exact matches , but somehow it is successful, since users prefer relatively short passwords which are easy to remember [64].

3.2.4 Replay Attacks

Another name of replay attack is reflection attack [65]. When a hacker detects secure network communication, intercepts it, and then resend it (or "replays" it) as if it was his own. This class of attack involves the leak of data unit and its transmission to obtain an unauthorized effect, to reuse message to cheat other [66].

3.2.5 Phishing Attacks

Hacker redirects user to the fake website to get the user authentication details [67]. For example if user desires to open a website says www.facebook.com, the user is diverted to a different website by the attackers, i.e. www.faceboOk.com whose interface is same as the original one, and user enters his username and password, without knowing that he has entered in the correct website. The

hacker/attacker then redirects the user to the original website by stealing his login data from the fake one. Phishing frauds have been getting large scale importance because these types of attacks have been climb in numbers [68].

3.2.6 Key loggers

Key logger is a computer software program, that records user activates in various ways i.e. screen, voice, keyboard, mouse and keyboard logging in invisible mode [69]. Attacker installs the key logger software on user computer system, the software creates a log file that keep track and send the log file to the attacker's email address with all the user's pressed keys, through which he can get the login data and can access the use important files [70].

3.2.7 Guessing Attacks

Guessing attacks always remain a serious threat [71]. Here an attacker performs repeated login trials by guessing possible values of the user password. Use of CAPTCHAs [72] can give a good defense aid for graphical as well as text passwords.

3.2.8 Smudge Attacks

Cell phones contain different kind of touchy individual data, for example, messages, notes, applications, music, pictures, thus substantially more. Despite the fact that it is extremely an extraordinary comfort to have these data in our cell phones, it additionally permits security chance if the majority of the data is effectively available. One approach to maintain a strategic distance from and keep the security assaults is to set some kind of screen lock, which gives validation on our cell phones [73]. To unlock a cell phone, user draws a retained unlock pattern with a finger on the touchscreen while the finger leaves its slick buildups, called smudge, shown in figure 3.2 on the surface of the touchscreen. The smudge can be abused by an unauthorized user to recreate the mystery design [74].

3.2.9 Electroencephalography (EEG) signal

Electrocardiogram (ECG) signals are one of the most significant biometric features produced by the electrical activities of the human heart [75]. By drawing the pattern of the user trying to imitate user's electroencephalography (EEG) signal, an intruder might try to gain access to the mobile

Figure 3.2: Smudge left on the screen

phone. This is done with the headset of EEG, the pattern is drawn and the machine is deceived to allow mobile device access [76].

Table 3.1 illustrates attacks on mobile touchscreen devices.

3.3 Password/PIN and Pattern Authentication

Text passwords are still common because they offer a number of benefits. They are simple to learn, enforce, and adjust if they are corrupted or forgotten, and they are extremely reliable. Unfortunately, the widespread use of text passwords across thousands of modern user accounts has made the task of creating and remembering a unique and random text password for each account cognitively impossible [77].

PIN/Password and pattern authentications are the most common authentication that exist by far. These approaches are vulnerable to classic attacks like guessing the attacks and surfing the shoulder [78, 79]. Other MPAS schemes, such as fingerprint and face recognition, are used to complement passwords, but they are not intended to replace them. Biometrics, according to security experts,

Table 3.1: An overview of attacks on mobile devices

Type of attack	Reference
Shoulder attack	[59]
Brute Force Attacks	[62]
Dictionary Attack	[64]
Replay Attacks	[65]
Phishing Attacks	[67]
Key loggers	[70]
Guessing Attacks	[71]
Smudge Attacks	[73]
Electroencephalography Signals	[76]

make it easier to enter systems; on the other hand, passwords are used to create initial trust and as a backup if biometrics fail [80]. DRAW-A-PIN authentication scheme is a suggested way of further improving the pin system [81]. In this authentication scheme a user needs to draw the pin code on his mobile screen instead of simply typing out his pin code. When a pin is drawn, the authentication system will first verifies the digits entered, and then observes the behaviour of the user used to enter the pin.

Authentication based on patterns is also a very common form of authentication today on many mobile devices [82]. Many users prefer it to PIN or text-based passwords because psychological studies indicate that visual content is learned and recalled better by the human brain than letters and numbers [83]. Pattern unlock is quite vulnerable to attacks like shoulder surfing and smudge attacks. People choose simple and easy pin/passwords and pattern to get authenticate because these schemes are easy to use and available in almost every mobile device.

[84] proposed a CAPTCHA AI hard problem-based salted challenge-response MPAS. The proposed framework based on the same principle as CAPTCHA. i.e., a bot's ability to recognize ed text in a picture is a difficult problem. By the use of client's password the framework combines the challenge text and scatters with in a random image, rather than submitting it in a way humans will find it easy, but bots will find it prohibitively difficult.

3.3.1 Password/PIN/Pattern Authentication Opportunity

It is not necessary to use the direct password input technique. In social engineering attack scenarios, the attacker can observe the user's behaviour, including password entry operations, while

the user is operating his/her mobile device. All types of display information, including user guide material, should be masked against new attack types if the methods entail direct password input procedures. The best approach to achieve this is to create a password entry method that isn't direct. When using indirect input, guessing all of the information from the shown data is quite challenging. As a result, regular PIN codes can be used in combination with an indirect input mechanism to allow personal identification and authentication.

3.4 Keystroke authentication

The use of keystroke dynamics has advanced over time and is now used in mobile phones. The main problem with cell phones, however, is that they can be used in any place. As a result, examining the utilization of keystroke dynamics using data obtained in different typing positions becomes essential [85]. Keystroke elements is a successful conduct biometric authentication for user validation at a work station [86]. Several research works have been done for MPAS by using keystroke techniques [87].

Khan et al. [88] test the vulnerability of keystroke dynamics on smart phones to password stiffening and mimicry attacks. They use feature analysis on a publicly available dataset [89] to create interfaces that teach users to mimic their victim's keystroke behavior and propose two schemes for an attacker to get real-time guidance when performing a mimicry attack. Against a number of passwords, their setup effectively circumvents keystroke dynamics. The researchers perform experiments to demonstrate how malicious insiders can use social engineering to gather keystroke data and then use that data to recreate the victim's behavior.

Buchoux and Clarke [90] use keystroke user authentication scheme and designed a software which can be run on Microsoft Windows Mobile 5. They proposed two types of passwords: a strong alphanumeric password and a simple PIN. Three classified were also evaluated namely Mahalanobis distance,FFMLP and Euclidean distance. Their results suggested that as PIN increased number of input data so performance of the defined classifiers was better when password was employed. People normally use either a pin or pattern to unlock their cell phones. The simple PIN schemes proposed here are always been prefer by the users being too short and easy to use.

Saevanee and Bhattarakosol [91] proposed a new mechanism for MPAS, named as finger pressure, combined it with inter-key features and existed hold time. To measure the finger pressure, users used touch pad of a mobile, acting as a touchscreen. Results shows 99% of accuracy, as this system doesn't require to remember any complex passwords or pin, just a simple password combines with

user's behavioral manners.

S Zahid et al.[92] examined keystroke data produced by 25 mobile devices users. The proposed mechanism takes a total of six characteristics of keystroke. These characteristics of various users are scattered and a finicky classifier is being utilized for the classification and clustering of the data. The proposed system has a error rate of 2% which indicates its a user friendly system and can be adopted.

Hwang et al.[93] suggested MPAS using the keystroke dynamics, that depends on a four digit PIN. Normally a four-digit PIN, can't give secure authentication, and are vulnerable to guessing and shoulder surfing attacks, so to make it more secure the authors introduced an input scheme supported by tempo cues and artificial rhythms. Their experiment work shows that the proposed technique reduces the energy efficient ratio from 13% to 4%.

Table 3.2 summarizes the keystroke authentication schemes.

Table 3.2: Summary of Keystroke authentication schemes

Reference	Year	Findings	Limitations
[88]	2020	Experiment with 30 people to configure over 400 mimicry attacks	Did not collect data from victims over the span of several sessions.
[92]	2009	A user identification system that detects a cell phone user's keystroke dynamics to identify authorized users from imposters	Not tested on BlackBerry category of phones that have QWERTY keyboards
[90]	2008	Low computational requirements that can be used on a real computer have been shown by statistical classifiers, with faster response in both template generation and sample verification.	Not tested on windows based mobile
[91]	2009	Learn the potential of person behavioural biometrics, including finger pressure, hold-time and inter-key	Small number of participants were used for experimental study
[93]	2003	keystroke dynamics-based authentication (KDA) provides better security against different attacks	comparison research of various mobile devices is needed to enhance the usability

3.4.1 Keystroke Authentication Opportunity

Mobile and portable devices have become increasingly common in people's daily lives as technology advances. In comparison to a few years ago, smart phones and tablets have ever increasing memory and processing power. Furthermore, advanced and sensitive micro hardware sensors, such as multitouch screens, pressure sensitive panels, accelerometers, and gyroscopes, have the ability to unlock new feature data. This upgraded hardware is now widely available, paving the way for future research into keystroke dynamics on this platform.

3.5 Authentication using Behavioral features

Researchers have proposed to use behavioural touch MPAS as a second line of defense if initial authentication is compromised [94, 95] or as center for the user who do not configure any of the authentication technique due to usability issue [96]. Behavioral authentication is a form of biometric authentication that has two benefits: first, it is implicit, ensuring it is done unconsciously. Second, behavioral characteristics are difficult to mimic because it is difficult for others to learn and replicate a person's behavioral habits after they have been established [97]. Behavioral biometric information i.e. touch gestures, mouse movements, and key strokes can be gathered via sensor devices and can be helpful to analyze the user's behavioral attributes for authentication [98]. In government departments, passport offices, border surveillance, and many consumer devices, there is a growing need for privacy-preserving biometric authentication systems [99].

A biometric device can be divided into two categories based on the number of modalities used: unimodal and multimodal. unimodal biometric systems focused on a single identifier, depend on a single modality for authentication therefore they are easier to create. The authentication metric itself can be a single point of failure, a unimodal device faces challenges such as noisy data, poor recognition efficiency, less reliable results, and spoofing attacks [100], [101]. In comparison, a multimodal biometric system uses multiple or combined parameters (for example, face and voice features) and does not depend on a single feature, making it much more stable and difficult to break. It is more resistant to spoofing threats, has higher recognition rates, and has improved accuracy and reliability [102].

Machine Learning schemes can be used to build improved protection schemes for MPAS [103]. Machine learning techniques are highly successful in enhancing the protection of applications regarding the touch screen of mobile devices. The key advantages of mobile phone safety software training algorithms include the ability to recognize biometric and sensor information in order to

enhance protection of mobile phones [104].

Bo et al. [105] suggested the use of support vector machine (SVM) algorithm to create a classification model based on cell phone users' biometric behaviour. The classification model developed updates the SVM model by introducing new features found through self-learning in order to enhance classification accuracy. The results show that the proposed authentication scheme for identification is fast and accurate.

Song et al. proposed [106] a secure, easy and fast authentication framework built using multi touch devices for the use of physiological and behavioral biometrics by the consumer using K-nearest neighbor (KNN) and support vector machine algorithm (SVM). Legitimate hand geometry and compartmental knowledge of users are employed to create a one-class SVM and KNN classification model. The experiment shows that, although the proposed system uses small number of experimental subjects and analyzes a few movements, in nearly every case the KNN outperforms the SVM.

Ehatisham-ul-Haq et al.[107] suggested that the performance of the three user-authentication algorithms should be measured and evaluated by Bayesian network (BN), SVM and KNN. The classifiers were trained to create a mobile user MPAS scheme based on their physical behavior. The three classifiers' precision was compared. The solution proposed can not provide various rates of access when identified on the basis of their biometrics of actions.

Liang et al.[108] proposed convolutionary neural network (ConvNet) to predirect the user tap series and device usage behaviour. Sensor data have been collected as users communicate with the system on different applications, and a classification model based on ConvNet, SVM, and KNN, is established using sensor data. The solution suggested did not make the CovNet model more complex in order to obtain stable and better performance.

Muhammad Sajjad et al.[109] proposed a hybrid technology with two layers of security, the first layer integrates the palm vein, finger prints and face recognition and layer two takes these things along with face anti spoofing convolutional neural networks (CNN) based models to detect spoofing. After matching finger prints successfully it is checked on CNN based model for the verification that it's fake or real. Repetition of the same method with face and palm. Experimental results verified the efficient work of the system, conquering the constraints in the area of spoofing techniques.

The Dynamic Time Wrapping (DTW) has been discovered to strengthen the security of mobile devices [110]. For the MPAS, only a small number of DTWs were used. DTW was used to build a

scheme [81] that validates the user by observing how he/she draws a PIN on a touch screen rather than typing it. On the basis of PIN drawing behaviour by the user, the DTW algorithm is being utilized for the comparison and realization of the similarities between the two PIN drawing sample of user. The experiment's findings show that users' PIN writing behaviour can be used for person identification, and DTW can support the proposed model with a promising results. The proposed research uses a small number of experimental subjects and does not equate its findings to those of other classification algorithms.

With a major increase in the IoT environment, researchers have begun to use the accessible sensual data from IoT devices to modeling the behaviors of humans. Machine learning algorithms are workable to improve the protection applications related to the touch screens of mobile phones [111]. Behavioral biometrics using machine learning classifiers are more widely used for implicit and continuous authentication [112]. In the research on continuous authentication that was based on gesture behavior of the user [113], 30 features were extracted by the authors from the retrieved data by touch screens and using SVM and K-nearest-neighbors (KNN) algorithms a validation model was developed based on sliding gestures (top and bottom). The equivalent error rate (EER) of their proposed system lies between 0% and 4%. To improve the accuracy, multi stoke features is missing for big touch screen devices like tablets. Bo et al. [105] suggested utilizing the SVM to construct a classification model based on touch behavior biometrics for the users of smartphones. The developed classification model updates the SVM model by introducing new observed features through self-learning to enhance the accuracy of classification. The results show that the proposed authentication scheme is fast and accurate with regards to identification. The authors in [114] proposed neuro-fuzzy inference system (ANFIS) classifier for the security of smartphones with pattern passwords. ANFIS is used as behavioral features to construct a classification model. Some of the features like touch pressure and touch stroke interval were not considered in the proposed scheme. Alpar and Krejcar [115] suggested Levenberg-Marquardt ANN (LM-NN). ANN was trained by touch location data. The outcomes indicate that the authentication of LM-NN is stronger and quicker as compared to other classification algorithms. The limitation in the system is the amount of epochs required to train the networks. The intervals would have been narrower if the number of repetitions is increased, resulting in a higher FRR and lower FAR. Zhou et al.[116] suggested ANN back propagation (BPNN) to enhance the security of smartphones. Using thumb stroke behavior, BPNN is used to build an authentication method. The proposed classifier offers an improvement in security and usability compared to the keystroke dynamics model. On the usability and security model, this scheme is limited to reduce the complexity of a password. In order to build an enhanced pattern, the password authentication method uses touch locations as

biometrics. Researchers did not perform the feature reduction, section, and transformation of data prior to model training.

In some cases, machine learning algorithms are merged or combined with a traditional technique. For example, a scheme in [117] created an authentication classifier using a combination of SVM and RBF. The SVM-RBF classifier is designed on the basis of multiple facial attributes extracted from smartphone users. The outcomes indicated that the created classifier (SVM-RBF) is highly stable, uses slight space and the greater performance under various conditions. This solution lacks the ability to adjust to attribute changes of the user, such as aging. Changing attributes of the user especially facial hair change are missing in this scheme. In [118], the authors used three separate algorithms to construct three classifiers, for user authentication, i.e. SVM, DTW and KNN. These algorithms focus on creating a classification scheme for the identification of smartphones users that is based on user's physical activities. The verification and testing were carried out in order to choose the best classifier among the three classifiers. The results indicate that SVM's general performance in authenticating individuals in five distinct positions on smartphones is higher as compared to DTW and KNN. This approach only considers the behavior patterns but neglects the background features. This study did not examine motion and physiological sensors along with contextual authentication knowledge. Liang et al. [108] suggested a Convolutional neural network (ConvNet) to predict user actions of the tap series and device usage. The sensor data was collected on various applications as users interact with the system and by the use of sensor data formulated on ConvNet, SVM, and KNN a classification model is constructed. As a comparison ConvNet performs better than SVM and KNN. To achieve consistent and better performance, the CovNet model with more layers was not considered. Ilesanmi Olade et al.[119] proposed a scheme of protection required to approve a user's identity utilizing a variety of familiar characters tics which distinguish the user from other users in a virtual and augmented reality environment. Identifying the task comes first, followed by identifying the individual in the identification process. Machine learning was used to test 65,241 datasets regarding the movements of hands, head and eyes in or- · to develop a continuous biometric authentication system and achieved an accuracy of 98.6%. This technique focuses only on specific age group. For machine learning, Artificial Neural Network (ANN) is considered among the strongest algorithms for machine learning that has gained considerable attention from researchers and shows up in various forms [120].

Touch biometrics are becoming an enticing way for mobile device users to be verified [121]. In [122], Lacharme et al. implemented biometric dynamic features similar to the typical Android unlock patterns of the location of the finger, strain, finger size and accelerometer sensor, achieving

a final 15.0% EER for imitation attacks using a Hamming Distance-based matching algorithm.

Different machine learning classifiers are use to train the system and distinguish between a legitimate user and an imposter. convolutional neural network (CNN) was used in several studies [123–125] in a two-phase method. Firstly, the training of CNN for representations of writer-independent characteristics. Secondly, to differentiate between actual and forged signatures,training of a writer-dependent classifier (e.g., Support Vector Machine) the CNN features were used.

In [81], for the authentication schemes based on PINs through the utilization of handwritten touch biometrics was assessed by Nguyen et al. Their suggested authentication solution resolved few early cited disadvantages when users were asked to draw every PIN digit in succession by them. Using a biometric device that was constructed using 5 dynamic characteristics and a match algorithm depending on DTW, a final 4.84% EER was achieved.

By progressively utilizing an Adaptive Radial design Base Function Network,97% precision of author authentication by handwritten characters and numbers is accomplished[126]. The method is tested on 15 writers' characters and numerals.

In non-Latin languages with a variety of characters, a writer recognition framework for touch-sensitive mobile appliances was introduced [127]. Complicated time-exquisite algorithms such as Multilayer Perceptron, Support Vector Machine or Hidden Markov Model are also avoided by the authors. A limited number of stroke form prototypes are utilized with weighted Dynamic TimeWarping and a Look-Up Table to identify strokes in a character.

RNNs for authenticating handwritten signatures were used in [128]. The authors suggested a Siamese architecture depend on RNNs in their research for signatures comparison. Verification output hits 5.5% EER on an assessment dataset of 100 users, with the device being trained on 300 different users. RNNs being effectively relevant to temporal prototype arrangements and acquired through the accomplishment for the recognition of English and Chinese writers [129], using a bi-directional RNN depend on Long Short Term Memory (LSTM) Cells[130] with 99% accuracy among 150 users.

Murat Taukoran[131] suggested a logged off signature recognition scheme depend on vector characteristics of the Histogram of Directed Gradients (HOG). At Yildiz Technical University, handwritten signature images are collected from 15 individuals, with 40 samples each. Applying the Size adjustment and decreasing the noise procedures to entire signature images before the extraction of the HOG feature. Principal Component Analysis is practiced to the dataset concern to avoid loss of time for processing and to remove redundant functionality. Obtained dataset is utilized for

training Generalized Regression Neural Networks. As a result, utilizing the proposed approach alongside two-folded cross correlation, a 98.33% accuracy is obtained.

Table 3.3 summarize the behavioral authentication schemes.

Table 3.3: Summary of behavioural authentication schemes

Algorithm	Reference	Year	Findings	Limitations
SVM	[105]	2013	The suggested technique consumes less energy while presenting quick and precise authentication	neglects context features
KNN	[106]	2017	KNN has good efficiency than SVM in all cases.	analyzed small number of gestures
CNN	[108]	2018	ConvNet has the highest predictive accuracy the tap behaviour of the user than the algorithms compared	need many layers to reach features layer
CNN	[109]	2018	Three modalities for efficient identification and smart spoof recognition are used in the hybrid scheme	User need to carry extra device for authentication
DTW	[81]	2017	DTW is use to authenticate smart phone users by using pin writing behaviours	The proposed scheme is restricted to few subjects and does not include any form of assessment

3.5.1 Behavioral Authentication Opportunity

Data encrypting and profiling procedures should be performed on the server to reduce unnecessary energy consumption. Mobile devices should consume as little energy as possible and should only be utilised to detect or sense the owner's actions. Then, using algorithmic selection, a subset of the data retrieved from each sensor's raw data should be sent to the server. The server could profile and encrypt the data for authentication purposes before sending it to the mobile device using the selected data. When the data is received, the mobile device can compare it to the current user's behavior pattern.

3.6 Graphical Passwords Authentication

Initially, any MPAS necessitates acceptance of a secure system that is simple, versatile, and adaptable. The graphical information based MPAS is among the schemes of authentication that depends

Figure 3.3: Login indicator

on the remembrance of protected passwords. Researchers have found that graphical passwords are more memorable than textual alphanumeric passwords

Recognition-based, pure recall-based, and cued-recall graphical passwords are the three types of graphical passwords [132]. The correct selected images during the registration are recognized in a recognition-based authentication scheme. The procedure, however, possibly interrupted by phishing attacks, that misleads users for capturing the screenshots of their passwords. Another drawback to this scheme is the discovery of some pre-selected images that involves scanning several images regarding the password, making the operation time-taking [133]. Users need to recreate or draw something because the password depends on pure-recall authentication scheme. When a stylus is not used, the disadvantages of schemes depending on recognition are fixed by the schemes depending on pure-recall however vulnerable to misconceptions [134].

Since they automatically mimic human inputs, the systems depending on pure-recall are slightly exposed to social engineering,dictionary and brute-force than text-based passwords. Cued recall authentication involves the user seeing a specified picture and clicking on one or more predetermined locations in a prescribed sequence. In contrast to the complicated and real-world segment, preconceived click objects need clear, artificial images, such as cartoon-like images. The user is susceptible to selecting the image's hot spot, which would be easy for a hacker to guess [135].

A technique named as pass matrix [136], which consists four modules namely, image discretiza-

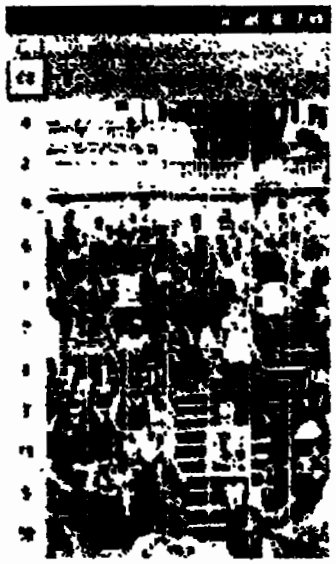

Figure 3.4: Login screen of pass matrix authentication scheme

tion, horizontal and vertical axis module, login indicator generator module and a communication module, gives a broad space for password to the user. This technique avoids shoulder surfing and smudge attacks. Login indicator will generate a new password for every session a dynamic pointer will be used by the users to identify the position of their password rather than clicking on the password directly. The user images are divided into 7-11 grid, smaller the image, larger the password space will be. Each time when the user will be login, he will touch the screen to see the indicator which can also be referred as a session password shown in figure 3.3.

The given indicator will be converted into an image which has horizontal and vertical axis repre-

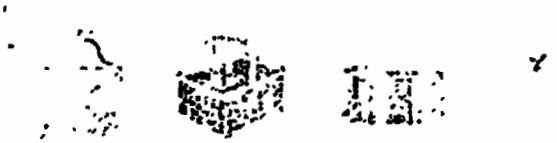

Figure 3.5: The target image from the degraded version of target image

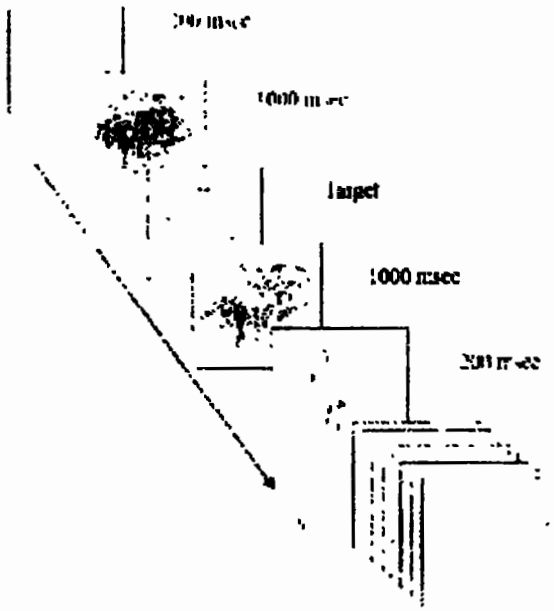

Figure 3.6: Degraded images and their masks

senting from A to G and 1 to 11 characters representing 7×11 grid respectively shown in figure 3.4. The module for password verification confirms the arrangement with in the pass square for each image. If the arrangement is accurate in every single image then the user will be permitted to log into the system.

Ashley A. Cain et al. [137] in their research concentrates on a series of graphics which are based on faster authentication while choosing the right images in 14 seconds. There are many distracting images from which the user has to touch or click the four target images. These series of images are comprised of low grade line drawings of daily life objects. The low quality or distorted unclear images are used to support cognitive object recognition. The system uses the Recognition by Components which tells us that 3D objects without the viewpoint of curving, linearity, shape etc. can be recognized. These graphics are made vague and unclear so that they become hardly identifiable objects shown in figure 3.5

At the same time, these nebulous graphics can be quickly recognized if the user is acquainted to the original object. Tainted images are shown on the screen for a very small fraction of a second, 200 milliseconds to be precise which is fast but authentic user will easily be able to cope with it. The degraded images are overlapped on each other to create a mask which stops for 1 second

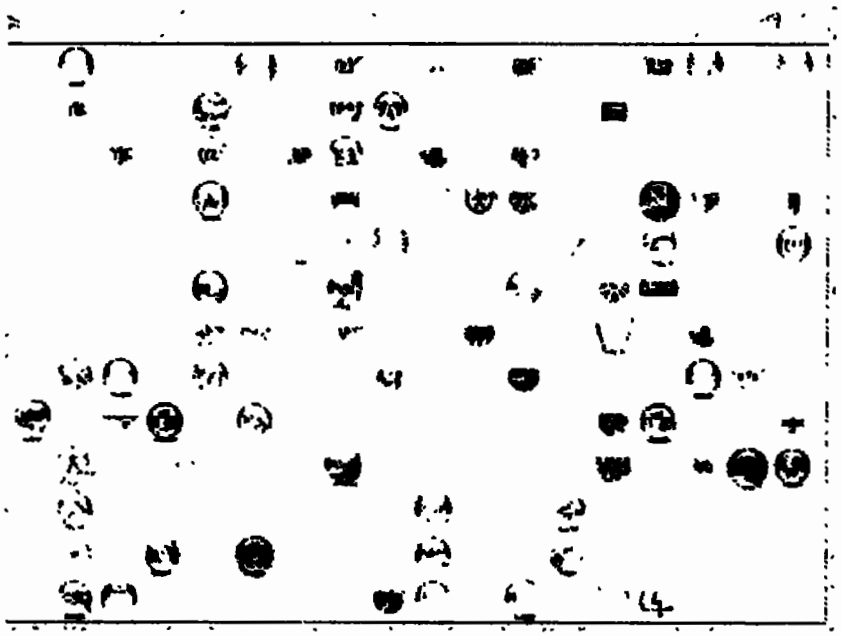

Figure 3.7: Example of a convex hull with three pass-icons

and comes after each degraded image shown in figure 3.6. These degraded pictures are shown randomly in between 7 distracting masks. The target image which is the correct one is not shown in the beginning to provide user time to fine tune to the streaming speed.

Irfan et al. [138] suggested a graphical password scheme based on text. Out of sixteen random images, the user selects five images. The arbitrary images shown are a mixture of graphical and text-based images being in password creation. This scheme 's login process consists of a 4 x 3 grid in which the last vertical grid shifts continuously. If the selected moving grid image is matched with the other two selected static grid images, the user can tap the image to activate the unit. The drawback of this schemes is the waiting time for the synchronisation of images that results in increased login time.

3D graphical passwords have introduced a new methodology for user authentication on mobile devices. Unity 3D package [139] is use to create the 3D graphical password and a device name Leap motion with the help of a scripting tool c# which allows user interaction with mobile devices. 3D graphical methodology is in the shape of cube matrix which consists of nodes and edges to construct the user password. This cube has eight green cubes of same structure; the user hand movement can be seen by the leap. The activity by the hand of the user within the observation

Figure 3.8: An example of a 3D graphical password created by the user

area, the 3D virtual hand will represents the users hand movement, which permits interaction of user with objects as shown in the figure 3.8. The positions of the cube can be randomly set. When the user touches any cube, it changes its state into visible manner. The arrangement of the being touched meant to record and pass through an algorithm to creates a unique password for every login.

Table 3.4 summarize the graphical authentication schemes.

3.6.1 Graphical Authentication Opportunity

A countermeasure could be the development of a non visible user graphical password authentication mechanism. Graphical elements are usually prominent. As a result, when compared to text-based passwords, graphical passwords may be more vulnerable under certain circumstances. An image is larger than text, assuming the graphical password using user predefined picture selection method, however a shoulder surfing attacker may have problems acquiring the original password from a long distance with a text-based password. As a result, a shoulder surfing attacker may obtain the password from a considerable distance. As a result, one or more authentication measures must be used in conjunction with a graphical password.

Table 3.4: Summary of Graphical authentication schemes

Reference	Year	Findings	Limitations
[140]	2005	Graphical password provide more security against different attacks	vulnerable to hotspot
[137]	2016	Degraded images are used for authentication that decrease the login time to 14s	The proposed study uses limited number of users for user study
[141]	2006	The framework helps a user with the easement regarding verification of the graphical password in an endangered environment as user indirectly selects the images for his password.	additional icon should be created to make the security settings more realistic
[139]	2016	3D graphical password for mobile authentication	usability of the scheme is not addressed
[138]	2018	Combination of text and graphical password	Waiting time for the synchronization of images results in lengthy login time

3.7 Summary

User authentication has been used for a long time to make sure that only the authorized user gets access to particular resources.User authentication systems come in static and dynamic varieties. Dynamic authentication validates users whenever they interact with a device, while static authentication only validates identities once. The majority of knowledge-based or token-based authentication systems, or systems that rely on what a user knows or has, are used with static and dynamic authentication. [142] Since knowledge-based methods and token-based methods are now the two most widely used strategies for user authentication, they make up the bulk of static and dynamic authentication systems. Knowledge-based approaches rely on user knowledge, such as a PIN or password, while token-based approaches rely on user possession, such as a key or magnetic card. Both of these approaches have several security problems. For instance, smart cards and passwords can be cloned, lost, stolen, or shared. The use of biometric authentication is another emerging technique. It uses physiological characteristics to verify users. Physical human traits are more harder to falsify than security codes, passwords, or hardware keys, making biometric authentication very trustworthy.Five modules are often used in the implementation of a biometric system: a

sensor module, a feature extraction module, a matching module, a decision module, and a system database module. Biometric systems often need to be validated on two aspects: user acceptance and system effectiveness. Due to human variability, a biometric technology cannot guarantee 100% accuracy. This fact emphasises the need for a user satisfaction and acceptability evaluation.

Chapter 4

Methodology

Text passwords are the most often used type of user authentication, however they have security and usability issues. Biometric systems and tokens, for instance, have their own set of disadvantages. Graphical passwords are another option, and the focus of this study along with behavioral authentication. Blonder was the first to define graphical passwords in 1996 [143]. In general, graphical passwords are divided into two types: recognition-based and recall-based graphical approaches. The user is shown with a series of images in recognition-based approaches, and the user passes the authentication by identifying and recognizing the images selected at the registration stage. The user is requested to regenerate something that was generated or selected by the user earlier during the registration process in the recall based graphical password. The problem with knowledge-based authentication systems is that they often use well-known text-based passwords [144]. Users frequently create memorable passwords that are easy to guess for attackers, whereas strong system-assigned passwords are harder for users to remember. Password authentication process encourages the use of strong passwords while still allowing them to be remembered. It is proposed that authentication mechanisms allow users to choose between using strong passwords and weak passwords. The task of choosing weak passwords is made more difficult in the system, which discourages users from doing so. With the introduction of smartphones and tablets, the graphical pattern unlock authentication scheme use to unlock mobile devices have become the most popular authentication scheme. [145]. With *something user process factor* the user will draw a new pattern at every login attempt. Behavioral authentication will give an extra security level in such a way that when a person interacts with a device like a tablet, smartphone, or computer, behavioural biometric authentication is used to identify them based on unique patterns exhibited.

Recent advances in authentication schemes attracted academia and market towards it. This thesis explores the research challenges related to following research questions.

"How the shoulder surfing attack can be avoided and what measures should be taken to measure the accuracy and usability of the authentication scheme"

4.1 Attack Model

This research focus on the two major threats on mobile authentication system, i.e. Shoulder surfing and smudge attack. Shoulder surfer attack occur when an bystander steals a pattern or pin code in a public place. Pattern lock, or PIN code to unlock the mobile device can be clearly observed on the screen. The lock pattern or PIN code can be instantly recognised and remembered by users, but attackers might be able to copy it with a casual glance as shown in the figure 4.4

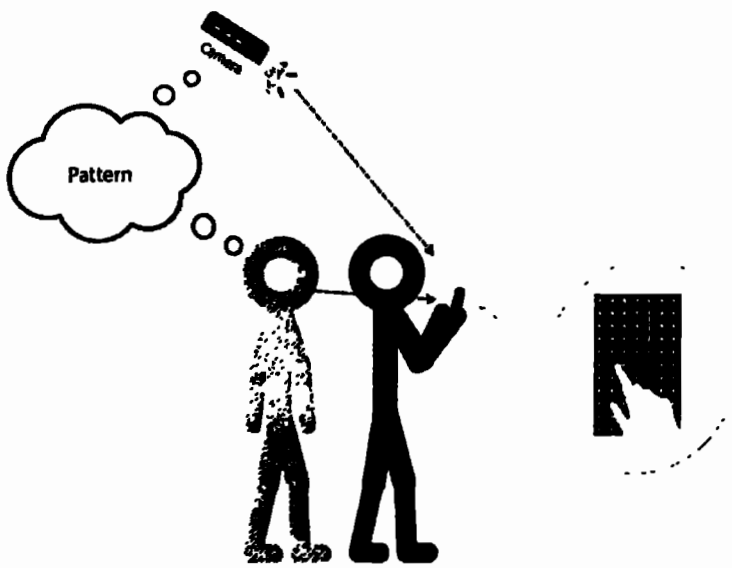

Figure 4.1: Shoulder surfing attack: Adversary try to obtain login information by visual means

A smudge attack uses greasy residues or smudges on the screen to obtain the password or unlock pattern of the mobile device. The strategy was explored by a group of researchers at the University of Pennsylvania [146]. Figure 4.4 illustrates how an attacker can quickly determine the user's pattern by analyzing the smudge left on the touch screen.

In this thesis we have proposed techniques that can overcome the threats associated to the above

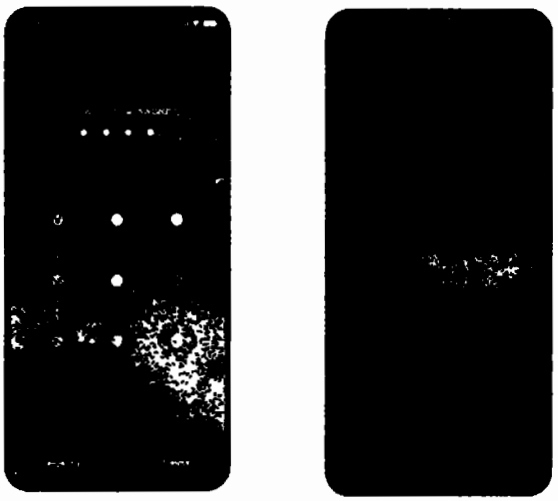

Figure 4.2: Sample pattern and its smudge showing connecting nodes of pattern

mentioned attacks, by adding a multi factor security of biometric features. At the authentication phase, not only the correctness of the pattern or PIN codes will be checked, but also the biometric features associated with the specific user will also verifies the valid user.

The proposed attack model is represented in the figure 4.3. An attacker by gaining the login information either by shoulder surfed or smudge attack will try to be loin on the mobile device of the user. The proposed system are designed in such a way that it does not allow the server to store a static pattern/PIN codes of the user as it changes at every login attempt. Even if the attacker have the knowledge of how to generate the pattern/PIN he/she has to mimic the be behaviour of the authentic user.

4.2 System Model

This section discusses the general working of the proposed models. In the registration phase, the user will register with the system by entering the required credentials. During the authentication phase, the user will process his pattern or PIN digits before drawing it on the screen. The pattern or PIN digit drawn by the user will be checked by the database. The user will be authenticated if the pattern drawn by the user is verified by the database and his behavioural features match with the behaviours in the feature extraction module. The system model is represented in the figure 4.4.

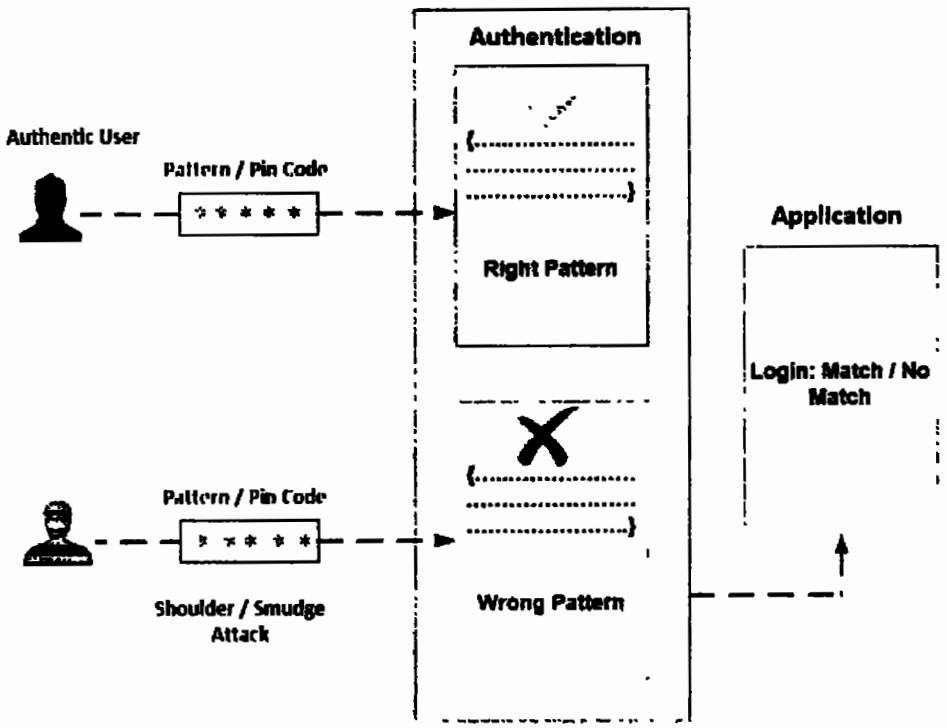

Figure 4.3: Proposed Attack Model

4.2.1 Data Collection and Feature Extraction

To begin with, data collection is a vital process for gathering specified features for the entire authentication process. The obtained data can then be used to create a specific behavior model with the help of appropriate classifiers. The selected classifier is supposed to aid in the detection of behavioural anomalies during the behavior matching phase by compering behavioral data to the typical model. Smartphones are equipped with a variety of sensors that may be used to detect real-world features such as user biometrics. The goal of this thesis is to see if we can learn an individual profile from a smartphone's touch behaviour while the user is unlocking the smartphone. The user will then be authenticated against unauthorised attackers using this model. The android application we created can collect behavioral data while the user is entering the password pattern or drawing the PIN codes on the touch screen. To get a sample of behavioural biometric data, participants were asked to repeatedly login to their mobile sets by drawing a pattern or a PIN on the touchscreen of a smartphone. While the user login to the mobile devices the touch screen and three built in sensors i.e magnetometer, accelerometer and gyroscope to gathered the behaviors data of the user. The touch screen event and these sensors collects the data, which contains the X, Y coordinates of finger position (fingerx, fingery), pressure (minimum and maximum) and slide angle

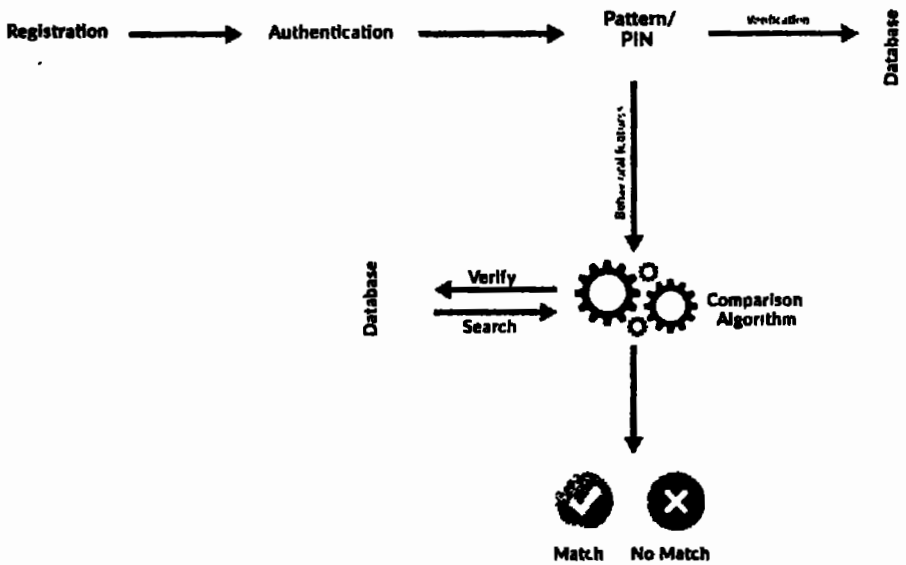

Figure 4.4: Proposed System Model

of finger from between points the nodes. Table 4.1 provides an illustration of the data. In order to properly login, the user must not only enter the correct password pattern, but also conform his behavioural features. By including behaviour authentication, it considerably increases the security of the password pattern.

Table 4.1: Example Data Collected from Touch Screen and Sensors

$Finger_x$	$Finger_y$	Min pressure	Max pressure	Timestamp	Slide angle
90	278	0.22362943	0.8	0.23333435	20
89	277	0.36872746	0.8	0.33334334	10
91	265	0.37284903	0.7	0.36666677	15
90	270	0.21583340	0.8	0.34444455	17
8[illegible]	274	0.36582201	0.7	0.32222211	12
90	254	0.35442104	0.8	0.35555577	16
91	254	0.35332104	0.8	0.32222277	16
90	254	0.35232104	0.8	0.36666677	16

To verify the user's authenticity, the data is collected by conducting an experimental study. In

this study, a mobile application was developed which extracts the behavioural data of the user at the time of login, and stores it on the server. The behavioural data includes the features listed in table 4.1. The gathered data was divided into two sets: training data and test data, to evaluate the validity of a user. The training data was gathered throughout 5 sessions. To examine the data, 3 sessions were held. The classifiers were trained to evaluate predicted performance using the test data set. For authentication, the collected data were analyzed by the server using the machine and deep learning models i.e. Support Vector Machine and Convolutional Neural Network. These models were implemented using python and the data was stored in CSV files.

4.3 Parameters

We explain our success parameter in this section. The following phrases are used to describe the outcomes of our evaluations:

1. **False Acceptance Rate (FAR):** is the percentage of negative users that were mistakenly identified as positive ones.
2. **False Rejection Rate (FRR):** is the percentage of positive users that have been unclassified as negative users.
3. **Equal Error Rate (EER):** is the point at which FAR and FRR are equal.
4. **Accuracy:** It's the proportion of appropriate assessments to all of them.
5. **Receiver Operating Characteristic (ROC) Curves:** The ROC is compared to the FRR and FAR. The ROC curve begins at (0,0) coordinates, passes through (1,0) coordinates, and ends at (1,1) coordinates. A greater performance is represented by a curve that is closer to the (1,0) coordinates.

4.4 Proposed Scenarios

This section discusses the different experimental scenarios to handle the research challenges discussed in chapter one.

1. ***How we can secure the authentication system from shoulder surfing attacks in public places or in office/home when someone is close by peeking?***

It's not always possible to avoid shoulder surfing. Simple measures such as using a privacy screen protector can help reduce the field of view on your screen, but they won't secure your keystrokes or pattern points while unlocking the device. We proposed random pattern and PIN entry authentication mechanism. At every login attempt user will draw a new pin or pattern, thus if the shoulder surfer observes two or more login attempts by the user, he will get a new pattern or pin every time.

2. ***Why a user should carry an extra device for the purpose of authentication?***

   Extra devices i.e. any biometric devices or card/tokens provide multi-factor authentication. But if the card/token gets stolen then the authentication key can be leaked out. We have proposed a model in which the user's behavioural characteristics along with the random password are checked by the server for authentication

3. ***How authentication scheme should be user friendly when it combines the graphical pad system with something user process authentication factor?***

   In something user process factor, user need to process some server given variables with his chosen variables (chosen at the registration time). The server will give unique numbers at every login session. We proposed a model in which user will do simple mathematical operation i.e. addition or subtraction. These mathematical operations are easy to perform by the users as this will be a single digit operation.

Chapter 5

Operation Grid (OP-Grid)

Passwords are the most commonly used method to provide secure access to user accounts. However, text and pattern passwords are vulnerable to different attacks like shoulder surfing attacks, guessing attacks and smudge attacks. To resist these attacks, this thesis proposes an OP-Grid technique; an implicit graphical authentication scheme having different patterns on every Login session. With a one-time Login pointer, the user creates his password pattern. A legitimate user is authenticated not only through the user-created pattern but also the way the user performs it using finger velocity and stroke time features. OP-Grid was implemented on android cell phones, gathered samples from 33 volunteers, and the experimental study carried out to evaluate its accuracy and usability.

Biometric techniques come under the category of "something you are" authentication factor and is divided into two approaches physiological and behavioral biometrics, it requires additional hardware (e.g. fingerprint scanners). In comparison, behavioral biometrics is used more commonly for continuous authentication [52]. Such methods, as the term behavioral implies, are focused on behavioral signals from the users, and authentication that occurs implicitly i.e. gait and touch dynamics are calculated by sensors. Authentication based on biometrics, differentiates individuals by their special biometric properties [147]. Unlike biometric technique, this work adopts "something you process" factor of authentication. Thus, this work proposed a multi factor behavioral pattern lock scheme. Firstly the user has to calculate the values of the pattern by using "something you process" factor of authentication. Secondly, the user has to draw the pattern, the user gets authenticated only if the touch dynamics features of the user matches the features saves in the system.

5.1 Contributions

The key contributions of this section are as follows:

- Developed an efficient and secure authentication system for consumer devices that can protect the user credentials in public places even in the presence of recording cameras
- Utilized the idea of "something user process", which allows the user to enter a new pattern on each login session, thus enhances the security against guessing attack, smudge attack, and shoulder surfer
- Proposed a multi factor behavior authentication method to strengthen authentication process in pubic places

5.2 Approach

To overcome the weakness of the pattern lock system the proposed scheme takes the fifth level of authentication factor and provides a graphical authentication system called Operational Grid (Op-Grid). As discussed earlier this factor of authentication requires the user to process a predefined formula to login into a system. OP-Grid consists of a graphical pad enclosed in a matrix of 7×11 grid with an image at the background that changes every time the module is called. Figure 5.1 shows the proposed OP-Grid. The creation of the resultant pattern is done by applying mathematical operations of addition and subtraction between the numbers selected by the user at the time of registration and the numbers given by the server.

OP-Grid is composed of the three components,i.e. Login Pointer, Password Verifier, and Feature Evaluation. Every time when the user enters a username, a login pointer will appear that shows one of the user's chosen alphabet and two random numbers between 1 to 5. Any communication between the user and system for authentication is protected by SSL(Secure Socket Layer) protocol and thus, is safe from being intercepted. The user processes the formula and draws the pattern accordingly to get authenticated. The password verifier module authenticates the user only if the result of the arithmetic operation is correctly aligned with the resultant pattern drew by the user. The details of OP-grid is explain in the next section.

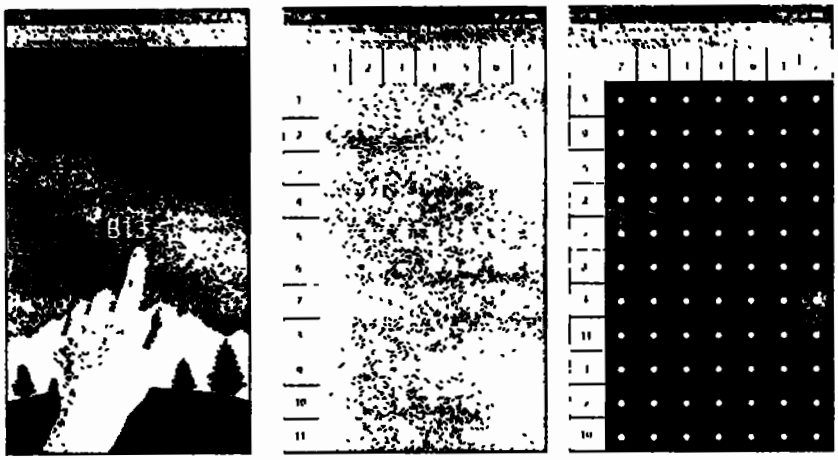

Figure 5.1: A visual way of login pointer and numbers of the horizontal and vertical bars generated randomly on every login to prevent shoulder surfing, guessing and smudge attacks

5.2.1 Registration Phase

First, the user chooses a username. The user selects two alphabets which are called Process-Alphabets(PA). The selected PA will hide the mathematical operation, the first letter will hide the addition operation and the second letter will hide the subtraction operation. The user also selects two numbers between 1 to 5, called Process-Codes(PC). PAs and PCs are used every time to generate a new password pattern by calculating them with login pointer number.

Working example: Assume that the username is Ali, PA is A, B and PC is (2,4). Alphabets of PA will be used to perform the mathematical operations of addition and subtraction i.e.

5.2.2 Authentication Phase

The user enters the username which was created at the time of the registration phase. A login pointer(LP) comprises of one letter from user's chosen PA and two random numbers between 1-6 will be shown. PA letter hides the mathematical operation. To provide a shield against shoulder surfing attack, the login pointer will be displayed to the user when he/she touches the screen of smartphones and will disappear when the hand leaves the screen. User performs that mathematical operation which is hidden in the LP of PA displayed letter i.e. either addition or subtraction, between the digits of user-selected PC and the digits of LP. User gets two numbers after performing the arithmetic operation, for example, it's 3 and 5. OP-Grid image of 7 × 11 grid will be shown, the user will draw a pattern from the third column to fifth row i.e. opposite L shape pattern. The

pattern drawn by the user will be checked by the password verifier. User will be authenticated if the pattern drawn by the user is verified by the password verifier module and his Behavioral features match with the behaviours in the feature extraction module. The server will display such PA's and PC's whose processed results will eventually be able to be inserted into the OP-Grid of 7×11.

Working Example: Let's suppose that at the time of registration user chooses Ali as a username, B and C as his PA's and 4,5 as his PC's. To login, the user enters his username, upon screen touch LP will be shown, which consist of one digit of PA, and two random numbers between 1 to 6. Assume that the PA letter is B and random numbers are 1 and 3, here B represents the addition operation. So the user will add the digits of his PC with the random numbers of LP i.e. (4+1) and (5+3) resulting in a pair (5,8) which represents a fifth column and eighth row of the OP-Grid image. User will draw a pattern of opposite L shape from the fifth column to the eighth row. This drawn pattern on OP-Grid image will be verified by the password verifier module.

5.3 Dataset: Collection and Training

This section explains the OP-Grid method in terms of obtaining touch dynamics from the touch interface and sensors, obtaining useful features from the extracted touch dynamics to identify users and what types of the classifier should be included. In current smartphones, numerous built-in sensors are mounted from which the sensor(s) that can accurately reflect the behavioral characteristics of the user was selected, while the OP-Grid pattern is being drawn. OP-Grid considers the touchscreen and three sensors that are commonly available in current smartphones: gyroscope, magnetometer and accelerometer. The touchscreen and these sensors represent different levels of information about the user's behavior. Table 5.1 shows set of smartphone sensors and their description.

Table 5.1: Smart phones embedded sensors

Sensor	Sensor Description
Magnetometer	Measures three axes (x,y,z) of the system geomagnetic sector
Accelerometer	Measurements of the acceleration force,including the gravity force
Gyroscope	Measures device rotation through three axes (x,y,z) with roll, pitch and yaw movements of the smartphone

33 students (14 females and 19 males) volunteered from our university to engage in this study. Among 10 out of 33 participants were assigned the role of attackers. Participants created an account with their unique username, PA and PC. After choosing the registration credentials the participants were told to get the login to the system in practise mode. They were asked to get login

with OP-Grid technique with their credentials for 20 days daily. The participants were told to get login using OP-Grid pattern for no less than 25 times a day. With this experiment around 40,000 samples were obtained from the participants. The actual values taken from the user weer labeled as 1, and the assumed values were labeled as 0.

Using machine learning techniques, from these samples the behavioral features were extracted that identify each sequence input as valid or imposter user.

When a user successfully logged-in based on the input of his OP-Grid pattern, then the information of user performing the pattern collected by the touch sensors would be stored as training sample; otherwise, the pattern will be discarded. Authentication of the pattern may be seen as a problem of classification. Legal users will be labelled 1 and illegitimate users will be labelled 0. Many researches [148] have implemented two classification algorithms such as SVM, Random Forest and Neural Networks to resolve classification issues. Table 5.2 shows the list of different features extracted from touch events and sensors user's OP-Grid pattern:

Table 5.2: Features extracted from touch events and sensors

Symbols	Name of Feature
T_{dr}	The time between touch down and touch release
T_p	Average touch pressure
S_{tp}	Standard deviation of touch pressure
M_p	Maximum touch pressure
M_{np}	Minimum touch pressure
S_s	Slide speed of finger from between points
S_a	Slide angle of finger from between points
N_s	Number of touch events of each segment
Avg_x	Average x value of each sensor
Avg_y	Average y value of each sensor
Std_x	Standard deviation of x axis value of each sensor
Std_y	Standard deviation of y axis value of each sensor
T_m	The maximum threshold time interval between two moving events to form a moving sequence

The features used in this research were used by the researchers [149], [150], [151] and ran different classifiers to achieve results. The description of the features is shown in table 5.3.

Table 5.3: Description of features

	Tdr	Tp	Mp	Mnp	Ss	Sa	Ns	Avg	Outcome
Count	623.000000	623.000000	623.000000	623.000000	623.000000	623.000000	623.000000	623.000000	623.000000
Mean	3.332263	0.385730	0.395602	0.076565	-0.630690	8.469775	2.689085	0.676273	0.491172
Std	1.342013	0.294822	1.095000	6.815491	4.106242	7.260671	2.052865	2.134881	0.500324
Min	1.000000	-0.5800000	-5.000000	-25.000000	-25.000000	-0.200000	-0.500000	-0.860000	0.000000
25%	2.000000	0.220000	0.100000	0.200000	-0.240000	2.000000	1.000000	0.147000	0.000000
50%	3.000000	0.360000	0.800000	0.700000	-0.110000	8.000000	3.000000	0.258000	0.000000
75%	4.000000	.0630000	1.000000	0.700000	0.400000	12.000000	4.000000	0.456000	1.000000
Max	6.000000	0.890000	1.000000	95.000000	0.700000	25.000000	8.000000	12.000000	1.000000

In this research we have utilize Correlation-based Feature Selection to access all the possible features. To evaluate a feature subset obtained from the Pearson correlation coefficient, Correlation-based Feature Selection uses correlation. This is a multivariate Feature Filter technique. That is, it evaluates many feature subsets and selects the best one [152]. The Pearson correlation map is plotted 5.2. This is a multivariate Feature Filter technique that is, it evaluates many feature subsets and selects the best one. The correlation coefficient is a single number that expresses the degree and direction of a linear relationship involving two continuous variables. The negative and positive correlation values of the dataset is shown in the table 5.4.

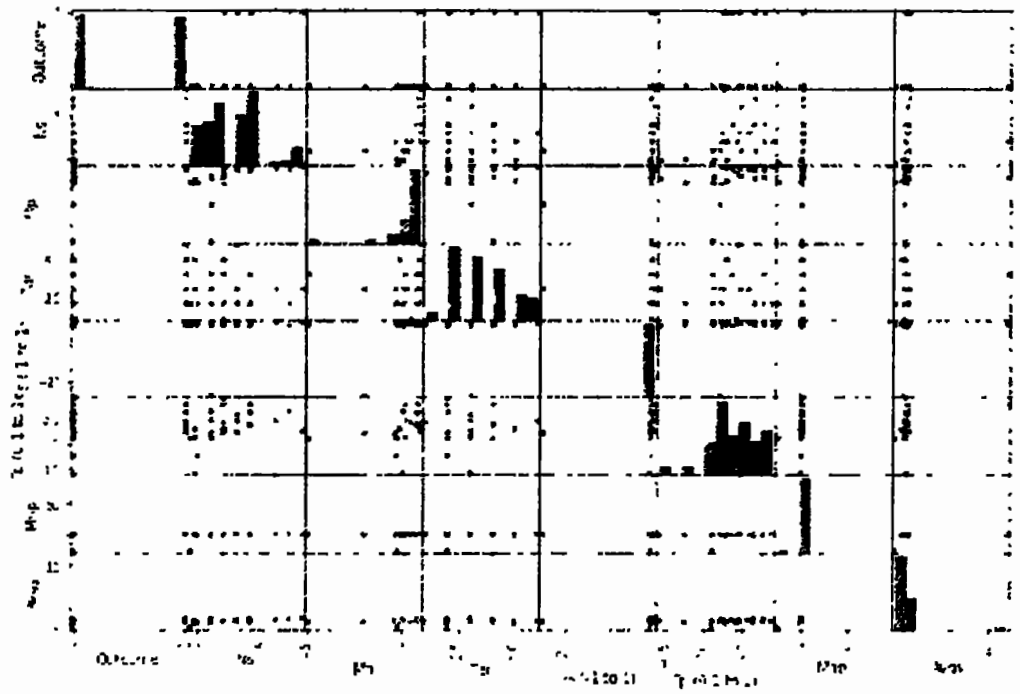

Figure 5.2: Correlation feature selection

The SVM classifier was trained based on the above features collected from different users, the collected data is served as training data and labelled as valid users(1). Once the algorithm is trained, it determines whether the legitimate user or some other user tried to login. Cross validation is used for the testing and training process. Cross validation uses all the data for the testing and training.

Figure 5.3 shows an overview of the proposed OP-Grid. The system consists of two components. The Op-Grid interface installed on smartphones. Once the user draws the pattern by using OP-Grid technique figure 5.3(a) it verified by the password verifier figure 5.3(b) if the password is correct, then it will move to the authentication algorithm of the user figure 5.3(c).

Table 5.4: Negative and Positive correlation values

Feature	Value
Outcome	1.000000
Ns	0.641993
Mp	0.481110
Tdr	0.359948
Sa	0.294419
Ss	0.203692
Tp	0.185577
Mnp	0.090284
Avg	-0.141422

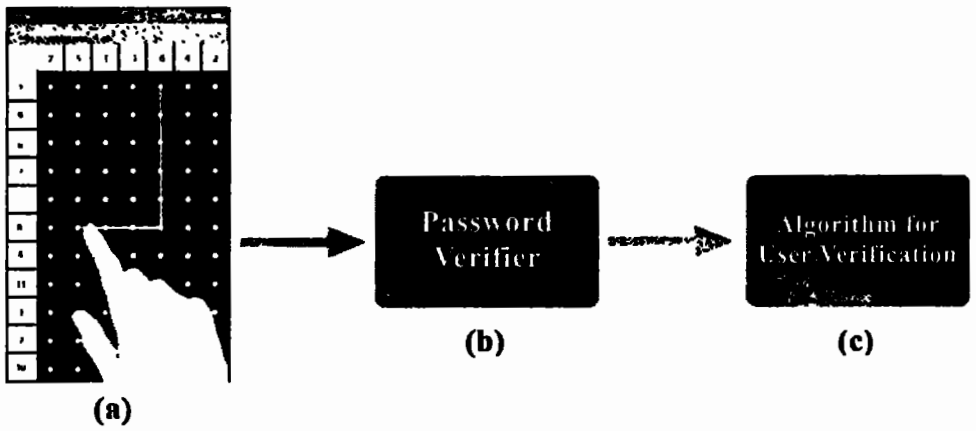

Figure 5.3: Three stages of OP-Grid

User authentication algorithm is shown in Figure 5.4, has two phases, the enrollment phase (training) and the verification phase (testing). In the former mode, the algorithm is fed with the true patterns labelled with their usernames i.e. patterns which are verified by password verifier. From these patterns, the system creates a profile of a user's pattern behaviour, which is required in the verification mode. In verification mode, the profile will be matched with the patterns from an unknown user. The algorithm will decide whether the drawn pattern has been performed by the legitimate user or not. The two classes required to learn the SVM are: first, the positive samples consisting of patterns from a valid user and second the negative samples consisting of patterns from all other users. Table III shows the comparison of OP-Grid with existing schemes that uses support vector classifier (SVM).

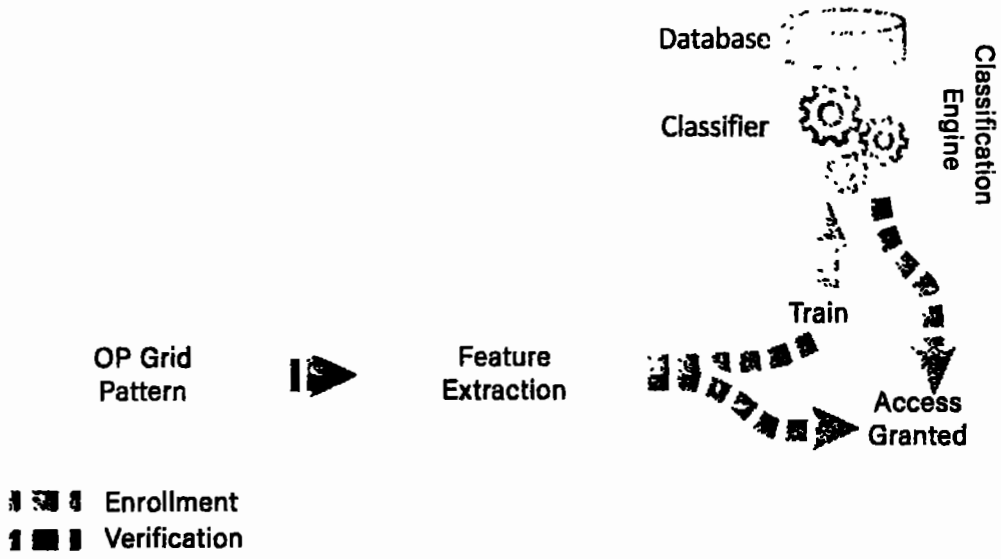

Figure 5.4: Data flow of the user verification algorithm

5.4 Experimental Results

Cross validation is used for the testing and training process. Cross validation uses all the data for the testing and training. We have run the data set using k-5 cross validation on three different classifiers i.e., SVM, DT and KNN. This study analyzed the two widely used performance parameters for mobile based behavior authentication systems, called false rejection rate (FRR) and the false accept rate (FAR). FRR treats authorized users as unauthorized users and denies the access and FAR treats unauthorized users as authorized users. Let's assume that No(A)da represents the Number of authorized user denied the access and No.(A)la represents the Number of authorized uses login attempts, the equation for False rejection rate is shown in (equation 5.1). Lets assume that No.(UN)aa represents the number of unauthorized user access approvals and No.(UN)la represents the number of unauthorized users login attempts, the equations for False acceptance rate is shown in (equation 5.2).

$$FRR = \frac{No.(A)da}{No.(A)la} \tag{5.1}$$

$$FAR = \frac{No.(UN)aa}{No.(UN)la} \tag{5.2}$$

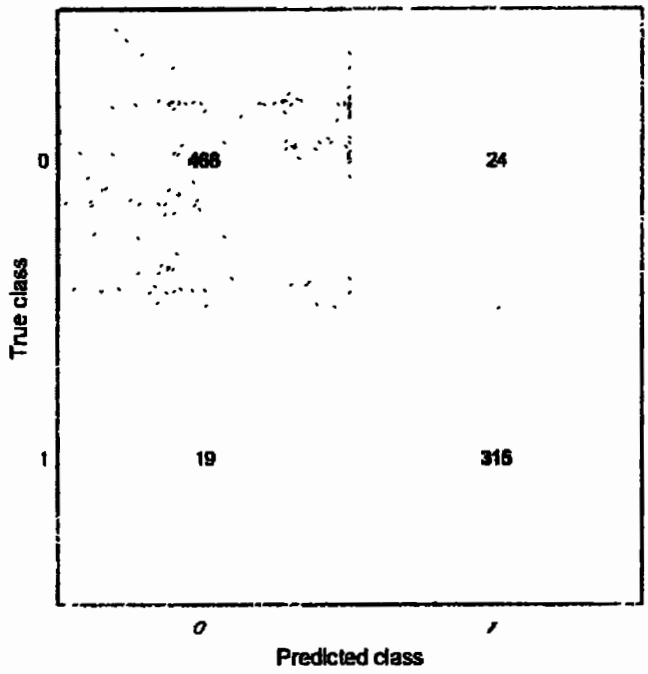

Figure 5.5: Confusion matrix of OP-Grid with SVM classifier

The confusion matrix figure 5.5 show the obtained true positive and true negative values, i.e., 468 registered users were correctly recognized as valid users, and 24 registered users were falsely recognized as invalid users. 19 unregistered users were wrongly verified as registered users and 315 unregistered were truly verified as non authentic users. The obtained results show the value of FAR 4.36 and FRR 5.03 and an AUC of 95% as shown in figure 5.6.

The dataset was run on different classifiers using k-5 cross validation technique and results have shown that SVM was the providing better accuracy then the others. The confusion matrix of the KNN and Decision Tree classifiers are shown in figure 5.7.

5.5 Security Verification of OP-Grid & Comparison

The OP-Grid is a 7 × 11 matrix, with an image at the background and numbers at the top of the rows and columns. The headers of the rows and columns change their position randomly at every login. This random position strengthens the security as the pattern of the user will not be at a specific row and column every time.

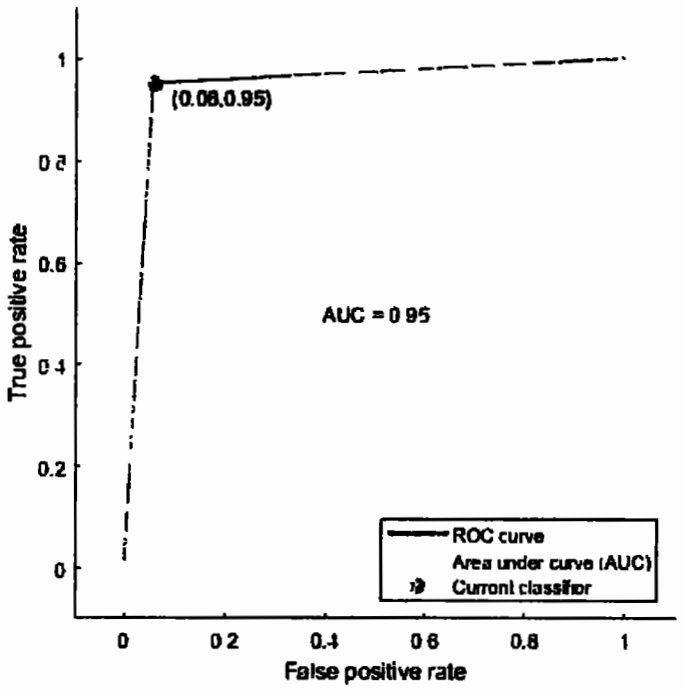

Figure 5.6: Area Under Curve graph of OP-Grid with SVM classifier

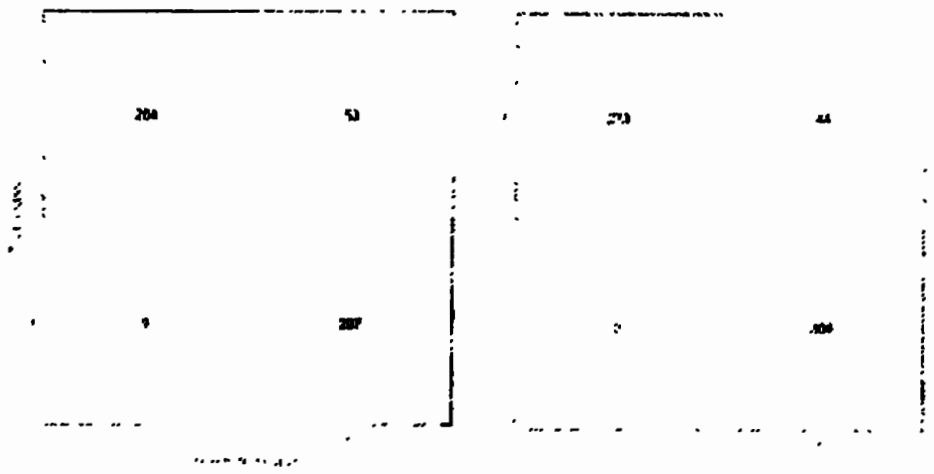

Figure 5.7: KNN and Decision Tree Confusion Matrix

5.5.1 Shoulder Surfing & Smudge Attacks

The pattern drawn by the user on every login session with small arithmetic operations of addition and subtraction makes the login process of OP-Grid very difficult for the shoulder surfer to catch. The attacker can not to see the login pointer generated by the server, as it disappears when the user removes the finger from the screen. If attackers try to login, then a new login pointer is generated, he will not be able to perform correct the arithmetic operation. Further, if the attacker records the pattern through the camera, still it will be an unsuccessful attempt, because the login pointer and the headers of the rows and columns changes values randomly.

For a test set, a total of 650 samples were used. An attacker has first to find the hidden values of PA and PC. Assume that he knows the PA and PC figures. Now he has to draw the pattern according to the user's behaviour. Four attackers have never been successful and some have been successful in few tries. In a sitting posture, the average rate of success of the attack was 3%. The results showed that when an attacker draws the OP-Grid pattern while walking, the shoulder surfing and smudge attack is not possible. Since, at the time of registration the choices of alphabets and digits is independent of each other for n choices,it gives

$$Total\ number\ of\ choices = \prod_{i=1}^{n} C_i \tag{5.3}$$

where C_i is the number of choices for position i,in our case which translate to

$$Total\ number\ of\ choices = \prod_{i=1}^{4} C_i \tag{5.4}$$

After using fundamental combinatorics, this quantity comes out to be 16900. The same idea can be applied to the authentication phase.

5.5.2 Comparison of Op-Grid

As shown in Table 5.5 SVM classifiers achieved better result as compare to others. The reason is that it depends on the problem, data size and features also; some algorithms work with some of the data or applications better than others due to the nature of the data and learning capabilities of an algorithm on that particular data. The value of both true negatives and true positives outcomes among the total number of instances evaluated is used to determine accuracy, display in equation 5.5:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{5.5}$$

The number of positive samples correctly detected by the classifier is known as sensitivity, and it is represented in equation 5.6

$$Sensitivity = \frac{TP}{FP + FN} \tag{5.6}$$

The number of negative instances properly detected by the classifier is measured by its specificity, which is determined by equation 5.7

$$Specificity = \frac{TN}{TN + FP} \tag{5.7}$$

The F-score is a measure of precision calculated from the recall (Re) and precision (Pr) conditions (equation 5.10).

$$Pr = \frac{TP}{TP + FP} \tag{5.8}$$

$$Re = \frac{TP}{TP + FN} \tag{5.9}$$

$$F - Score = 2 \times \frac{Pr \times Re}{Pr + Re} \tag{5.10}$$

where FN denotes False Negative, FP denotes False Positive, TP denotes True Positive and TN stands for True Negative [153].

Table 5.5: Performance base Comparison

Classifier	Accuracy	Sensitivity	Specificity	Precision	Recall
SVM	94.8%	96%	93%	96%	95%
KNN	88.1%	90%	87%	89%	90%
Decision Tree	93.2%	95%	91%	94%	92%

Table 5.6 present the comparison of Op-Grid technique with different authentication systems. [76] has used the SVM classifier for brain signal authentication, but brain signal across the network are limited. [113] uses SVM and found that SVM is more accurate then K-Nearest Neighbour, but fail to consider the attributes like position and accelerometer data. Op-Grid uses accelerometer data to measure the accelaration force put on the screen while drawing the pattern.

[105] proposed authentication technique using SVM classifier that requires less power for authentication. This techniques neglects the contextual characteristics that can affect the validity of the model. [118] suggested that SVM perform better in different mobile phone positions then Decision tree and K Nearest Neighbour, but has taken consideration only a few number of sensors. Op-Grid uses two factor of authentication i.e. something user process factor and pattern password to authenticate the user. The drawback of Op-Grid technique is that user draw a 90 degree angle shape pattern to authenticate at every login session.

Table 5.6: Comparison of related work

References	Algorithm	Findings	Limitation
[76]	SVM	The proposed SVM-HMM outperform the NB and cosine similarity	Authentication by brain signal across the network is limited to the proposed framework
[113]	SVM	The SVM is more accurate than the K Nearest Neighbour	The proposed authentication scheme does not take into account attributes such as position, accelerometer data.
[105]	SVM	The proposed approach requires less power and is authenticated easily and accurately	The approach proposed neglects contextual characteristics that can affect the validity of the model
[118]	SVM	The SVM performs better in different cell phone positions than the DT and KNearest Neighbour	The approach proposed examines only a number of sensors and does not take contextual information into consideration
OP-Grid	SVM	Two factor authentication using fifth factor and SVM classifier	User can draw only pattern of 90 degree

Table 5.7 present the comparison of Op-Grid technique with different authentication systems regarding security analysis. The comparison is based on Shoulder surfing, smudge attack, Spoofing attack, One time password, Biometric, and multi factor password system.

Table 5.7: Comparison of related work w.r.t Attacks

References	Shoulder Attack	Smudge Attack	Spoofing Attack	Multi-factor Authenti-cation	One Time Password	Biometric	EER/Accuracy
[154]	✓	✓	✓	✓	✗	✗	
[155]	✗	✗	✗	✓	✗	✓	EER=1.2%
[156]	✓	✓	✓	✗	✗	✓	Acc=95.01%
[157]	✓	✓	✗	✗	✗	✓	EER=2.6%
[158]	✓	✓	✗	✓	✗	✓	FAR=1.4% FRR=2.08%
OP-Grid	✓	✓	✗	✓	✓	✓	FAR=4.36% FRR=5.03%

5.6 Summary

The chapter carefully describe a novel graphical authentication scheme, OP-Grid, that is a combination of authentication factor "something you process" and behavioral features. The contribution of the OP-Grid scheme is that it provides a secured defense system having a check on every login session. The login pointer has a unique value, a feature that keeps headers of rows and columns change their positions. Further, the behavioral features of the user created during stored in the server during the training phase have a tendency of being unique. The protection of user credentials in public spaces, even when recording cameras are present, has been made possible by the development of an effective and secure authentication system. The major contributions of the proposed system as listed above ensures security even if an adversary is equipped with the a camera or tries to attempt shoulder surfing attack or smudge attack. This method can further be strengthen by including physiological and moving sensors for user identification. KNN, DT, and SVM are three distinct classifiers that we used. In terms of FAR, FRR, accuracy, f-score, precision and sensitivity and the SVM classifier beat the other classifiers.

Chapter 6

Processed Pattern Authentication

User authentication is one of the critical concerns of information security. Users tend to use strong textual passwords, but remembering complex passwords is hard as they often write it on a piece of paper or save it in their mobile phones. Textual passwords are slightly unprotected and are easily attack-able. The attacks include dictionary, shoulder surfing, and brute force. Graphical passwords overcome the shortcomings of textual passwords and are designed to aid memorability and ease of use. This chapter proposes a Process-based Pattern Authentication (PPA) system for Internet of Things (IoT) devices that does not require a server to maintain a static password of the login user. The server stores user's information, which they provide at the time of registration, i.e., the R-code and the symbol, but the P-code, i.e., the actual password, will change with every login attempt of users. In this scheme, users may draw a pattern on the basis of calculation from the P-code and R-code in the PPA pattern, and can authenticate themselves using their touch dynamic behaviors through Artificial Neural Network (ANN). The ANN is trained on touch behaviors of legitimate users reporting superior performance over the existing methods. For experimental purposes, PPA is implemented as a prototype on a computer system to carry out experiments for the evaluation in ٦٩ of memorability and usability.

Accounts whether they may be of emails, social networking websites, website administrators, personal computers, or networks, are mostly protected by passwords. Textual passwords are common in use methods of authentication. Memorization of powerful passwords is burdensome, thus, people normally choose short passwords or even simple dictionary words. The worst situation is that users may use the same username and password for multiple accounts for their easement, that make it more vulnerable, where the exposure of one password can lead to security breaches of all

accounts associated with it [52], [159]. Each Internet of Things (IoT) device and account must have a distinct password for security, if in case the attacker gets success for breaking a password, he cannot breach the other accounts. According to a study in [42], a security team at an organization ran a password cracker and amazingly cracked about 80% of the employees' passwords in less than a minute. It is advised that users must use long and complicated passwords that contains special characters, letters (upper- and lower-case letters), and numbers, to protect their devices from different attacks. In general, it's very hard to memorize complex and lengthy passwords. Consequently, for logging into different accounts users prefer to save the passwords by writing on paper that raises the likelihood for the violation of security by different attackers [160].

To tackle the weaknesses of traditional passwords, graphical password techniques were introduced. Graphical passwords such as OP-Grid [161], PassTag [162], and Passpositions [163] make cell phones more adaptable than the conventional, because a wide scope is offered for symbols over password techniques based on text. They are therefore being introduced in smart devices. The authentication process having multi-factors, e.g., "Something you Process", is used by researchers while presenting their schemes against attacks, such as shoulder surfing attack [164]. In such multi-factor authentication, users remember the equation/formula and the values of variables are given to them at the time of authentication. A user puts these values in the formula and processes/calculates the outcome in his/her brain, which is then entered as a password. The values of variables may change; therefore, the password changes every time it is entered. Hence, an attacker may know the password, which restricts user to login with that password.

With the adoption of the Android mobile operating system, a substitute to PIN authentication, known as pattern authentication system, on mobile devices has been implemented and widely deployed. A user generates a hidden authentication pattern on a 3x3 grid with his finger and then redesigns it for verification, as shown in Figure 6.1.

Compared to PIN/Password, authentication through pattern keeps the brain to learn the information and accumulates in a better way. The pattern might remember in the form of an image, thus manipulate the impact of illustrated supremacy [165]. Patterns are exposed to a hazardous environment, even if a user selects complex or lengthy ones, as in the case of shoulder surfing attack, where the adversary is capable to know what you have drawn as a pattern. Some of the attacks are discussed below.

- Shoulder surfing is the latest weapon used by hackers as this technique depends upon observation for example sneaking over the shoulder or recording his login or other information

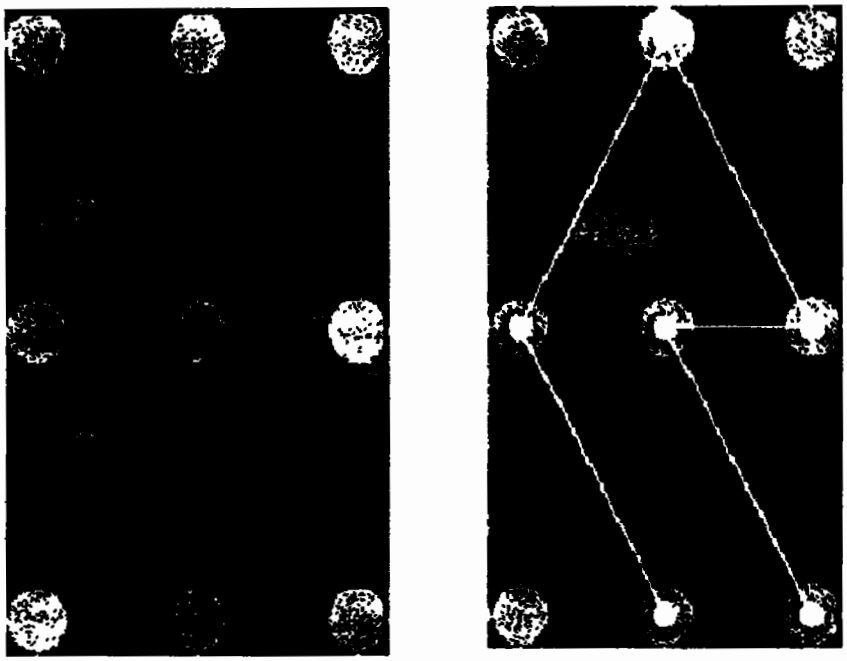

Figure 6.1: Standard layout of authentication system through pattern

by using a hidden camera. This type of attack is an effective way to steal the authentication data, i.e., pattern, as it requires no extra knowledge or software. Pretty much every "keen" customer's gadget today incorporates a camera, from savvy watches to shrewd TVs, glasses, telephones, and MP3 players. Researchers at Black Hat [41] exhibited that how these cameras can keep an eye on individuals tapping, for example, passwords or patterns into mobile and tablet consoles.

- Pattern authentication methods require users to touch the display screens for login and thus are vulnerable to smudge attacks. An attacker can retrieve the pattern of the users etc. through examining the marks remain over the display screen [166].
- In password guessing attack, a hacker can guess a user's pattern password using his stolen cell phone devices as well as the data caught during the registration or authentication phase [167].

We all have different "living credentials" such as fingerprints, facial expressions, optical elements, voice tones, and behavioral attributes. User behavior is one way to represent the identity of an individual [168]. It identifies whether the current user is a valid one by collecting and training the features of the sample data in order to carry out authentication. The key characteristics of

behavioral authentication are as follows:

- It is an entirely back-end application, ensuring that the whole data collection and authentication process doesn't require users to do something that sounds user-friendly.
- Additional hardware support is not required, it only needs a smartphone with common sensors and a touch screen.
- It does not overlap with other methods of authentication.
- It is hard to conceal but only possible if the attacker can accurately mimic the actions of the owner.

"Something user process" is an authentication factor [44], which is a formula-based authentication that requires the formula processing by the user that the server provides related to the numbers or images. This study suggests a multi-factor behavioral pattern lock system. First, by using authentication factor "something you process" the user shall compute the values for pattern. Second, the pattern will be drawn and validated if the user's touch dynamics features match the features saved in the system. Following are the primary benefactions of the study:

- Built-in effective, reliable authentication framework.
- Use the concept of "something you process" authentication factor that allows users to enter new patterns on each login session, hence, improving protection in opposition to shoulder surfers, smudge and guessing attacks.
- Proposed multi factor behavior authentication method using "something you process" factor, the drawn pattern by the user is checked, i.e., whether it is correct or not, later on by using the login behavioral features of the user, will conclude the correctness of drawn pattern.

Few of the authentication schemes are limited to specific age group [119], or are not compatible with large screen mobile devices [113]. The features like touch pressure and touch stroke intervals missing in [105]. The proposed authentication system in this chapter have tried to overcome these flaws. The concept of "something user process" is used, which lets the user to enter a different pattern for each login session, hence increasing security against guessing attacks, smudge attacks, and shoulder surfer attacks. Something you process enhanced the security that even the attacker mimics the behavioral features of the user, but cannot find the trace the exact pattern as the pattern is different at every login attempt.

6.1 PPA

This proposed technique addresses the weaknesses in pattern lock method by the implementation of the authentication's fifth factor and introduces Processed Pattern Authentication (PPA). As described earlier for login purpose this authentication factor requires the processing of predefined formula by the users. It uses a graphical pad comprising 10 graphical boxes, each having a combination of symbols and numbers used in the authentication process, as shown in Figure 6.2. Each graphical box in the graphical pad has 10 symbols representing numbers from 1 to 10. The user after calculating two digits of the process-code to get the pass-code will draw a pattern from one graphical box to another having the user's symbol and the pass-code digit. During registration, user's selected numbers is referred to as R-code (Registration code), and the server's given along with mathematical operation symbol to the user for processing along the R-code is referred to as P-code (Process-code), whereas the resulting password is referred to as Pass-code.

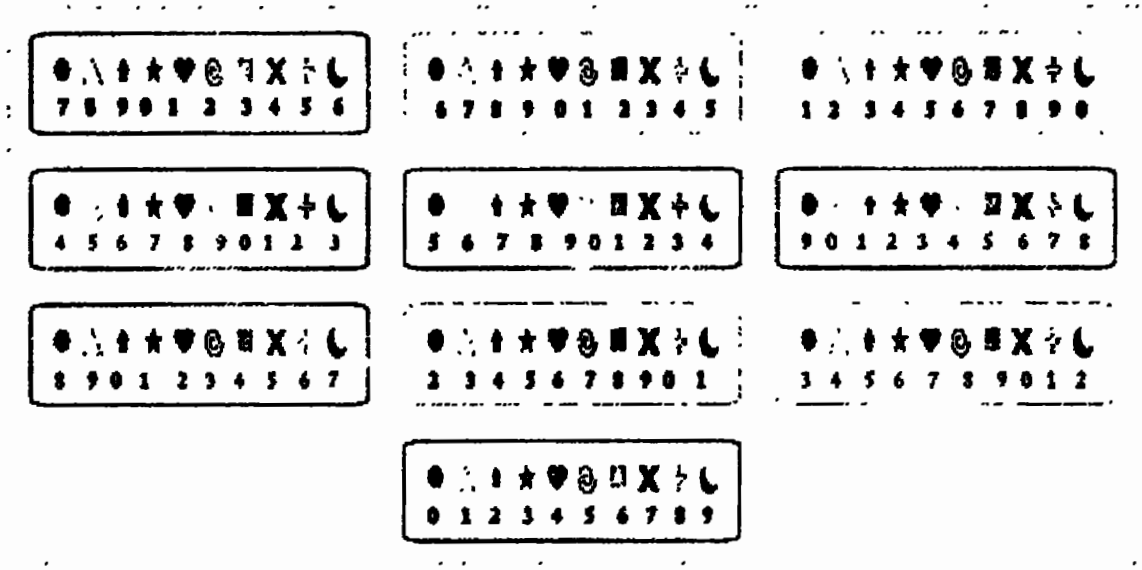

Figure 6.2: Graphical Interface PPA

The PPA comprises three components, i.e., the P-code Indicator, Pattern Checker, and Feature Extraction and Evaluation. The P-code Indicator displays two random numbers between 1 and 5 along with two alphabets for the addition and subtraction operations, which will appear every time during user authentication. The communications between user and authentication system is secured by Secure Socket Layer Protocol (SSL) [169]. After processing, the user will get two numbers and draw a pattern connecting two graphical boxes (having its symbol and the resulting Pass-code digits) in the graphical pad. The pattern checker module checks the validity of the drawn

pattern by the user. The pattern checker authenticates users on the condition that if the outcomes of the arithmetic operation between the R-code and P-code is accurately in position with the resultant pattern drawn by users. Once a user draws the pattern and finds it correct by the Pattern Checker, meanwhile by using machine learning model the pattern drawing behavior of user is examined. The PPA was installed on the user android smartphones, where the users were asked to use the PPA authentication pattern lock system around 30 to 40 times to obtain the training samples. A total of 29008 pattern samples were obtained from 35 users. The PPA has two phases, registration and authentication, subsections coming next provide description about the phases.

6.1.1 Registration Phase

In registration phase, following steps are performed by the user in a sequence

- Chooses a username
- Selects a symbol (from the given sets of symbols)
- Selects an R-code (minimum of 2 digits)

Once the three required credentials are selected, the registration phase concludes. A user inputs three things in the registration phase, i.e., username, symbol, and R-code. The server will keep the user R-code and symbol information against the username. Let us suppose that Ali is the user name and the triangle is the symbol. Let the R-codes chosen by the user are 7 and 6. The user will click on the box that has 7 triangles, as shown in Figure 6.3. The same will be done for the second number 6. When the user sees the pairing of his/her chosen symbol and the R-code digit, he/she can click anywhere in that box, which makes it nearly impossible for a shoulder surfer to guess any one of them.

6.1.2 Authentication Phase

...e steps for the authentication process are as follows.

- User enters his/her username.
- Graphical pad appears on the screen having different boxes with symbols and numbers.
- P-code Indicator will display two random numbers between 1-5 along with two alphabets either 'U' or 'R'. 'U' represents the addition and R means the subtraction.

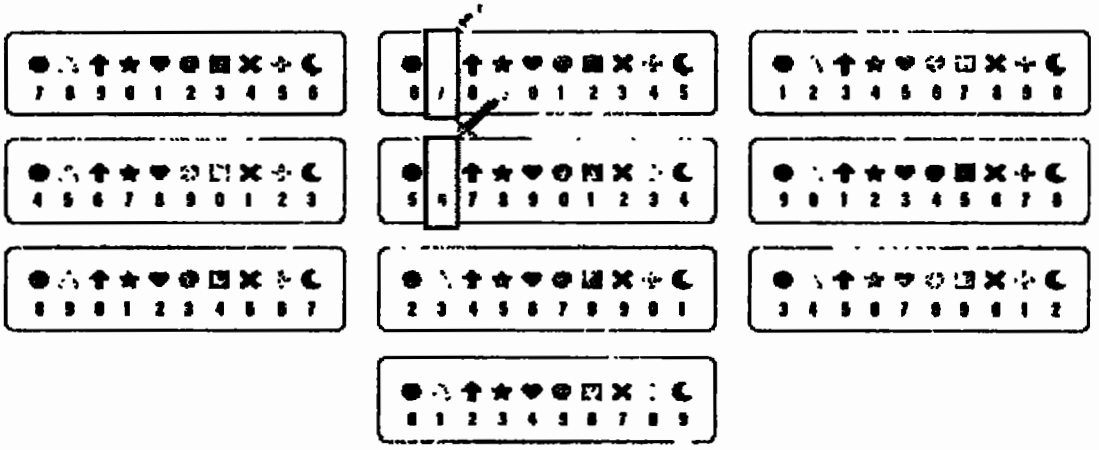

Figure 6.3: Registration example

- User will add or subtract the P-code digits given by the server taken from the R-code to generate the two Pass-code digits.
- User will draw the pattern between those specific boxes in the graphical pad that have resultant Pass-code digits under the registered symbol.

Suppose a user's R-codes are 1 and 4 and the symbol is a triangle. When he/she enters the username for authentication, the P-code Indicator will show the two process code digits to be added or subtracted from the two R-code digits. Let us suppose the first process code for the first R-code digit 5U, i.e., add 1 with 5, and the second process code for the second R-code digit is 2R, i.e., subtract 2 from 4. The resulting Pass-code digits are 6 and 2. The user will draw a pattern by connecting the nodes of two graphical boxes that have 6 and 2 written below the triangle symbol, as shown in Figure 6.4.

Feature Extraction

The PPA is a two-factor authentication technique, i.e., firstly authenticates the user according to the values drawn as a pattern, and secondly how he/she draws the pattern. Latest smartphones have numerous installed sensors that are built-in them where from the desirable sensor(s) is selected that is capable of representing behavioral characteristics of the user, while the PPA pattern is being drawn. A collection of smartphone sensors that have been used in various researches [82] [170] is

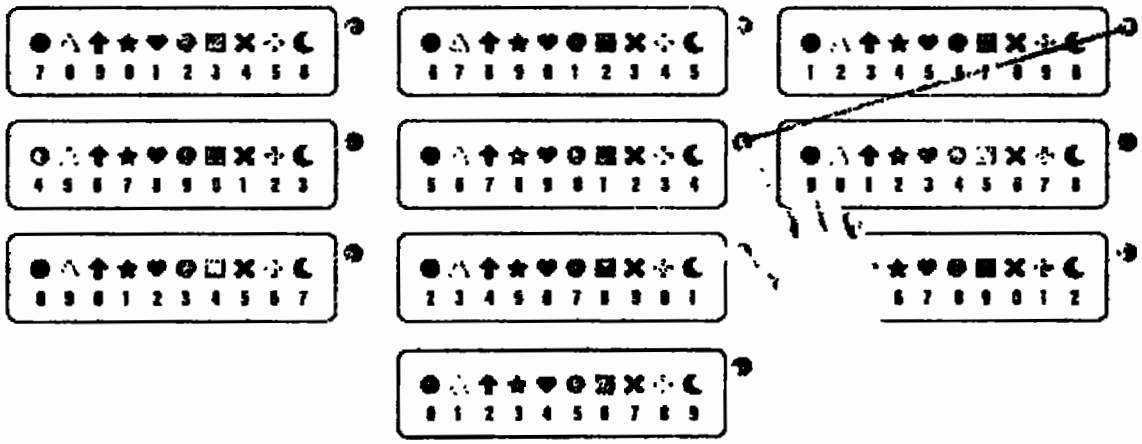

Figure 6.4: Login example

shown in Table 6.1

Table 6.1: Embedded smartphone sensors

Name of the sensor	Functionality
Linear Accelerometer	Computes the force of acceleration applied on the smartphone except force of gravity
Accelerometer	Computes the force of acceleration applied on the smartphone including force of gravity.
Magnetometer	Computes the geomagnetic ambient field on three axes (x, y, z)

The installation of PPA was done on the participants mobile phones who were asked to unlock a device using the pattern of PPA. After accomplishing successful log-in of the user that formulated on his PPA pattern input, later on the information is saved regarding the drawing of pattern by the user that is collected using the touch sensors in the form of training sample; else, rejection [illegible] drawn pattern. The pattern authentication can appear being a classification issue.1 and 0 are marked as Legal users and illegitimate users respectively. SVM, Random Forest, and Neural Networks have been introduced by several research studies as classification algorithms [171], [172] to solve the classification problems. The proposed scheme for two-class classification chose to consider Artificial Neural Network. The analysis of neural network simulations in biological neural networks highly inspire the mathematical model related to artificial neural network (ANN). Like human brains, the ANN strives to construct the way for the quick processing of data. Table 6.2 lists various features derived from touch and sensors of the user's smartphone while using the PPA

authentication system.

Table 6.2: The set of extracted features

Feature Symbol	Feature Name
T_{dr}	Time between touch down and release of pattern nodes
T_{ap}	Average touch pressure while drawing the PPA pattern
M_{xp}	Maximum touch pressure while drawing the PPA
M_{np}	Minimum touch pressure while drawing the PPA
M_{xp}	Maximum touch pressure while drawing the PPA
S_{ss}	Speed of finger sliding between PPA nodes
S_{sa}	Angle of finger sliding between PPA nodes
Avg_{ax}	Each sensor's average x value
Avd_{ay}	Each sensor's average y value
Std_p	Touch pressure's standard deviation

An overview of the PPA is shown in Figure 6.5. Two components make up the system. The smartphone is installed on PPA. Using the PPA technique when the pattern is drawn by the user figure 6.5(a), the Pattern checker module checks if the pattern is right figure 6.5(b), then it switches to the next level figure 6.5(c) of the user's authentication algorithm.

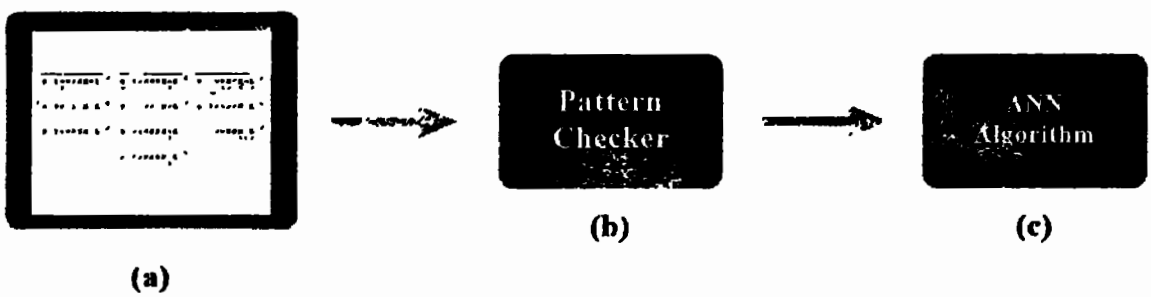

Figure 6.5: Three stages of PPA

6.2.1 Initialize Setting

The neural network is constructed in this step by specifying the design of the network (input units, output units). Features that are extracted from the touch and sensors of smartphone are utilized in

training the neural network.

6.2.2 Training Set Generation

The quality of learning is considered essential for the neural network, as it's providing the capability to the network in order to address the changes in the environment. For this objective numerous learning algorithms were developed. On the basis of the features (Table 6.2) gathered from various users, ANN is trained, the data that is gathered is used as training data and la-belled as valid users (1).

6.2.3 Creation of Neural Network

In this stage, a multi-layer network that contains multiple hidden layers is fed with the training set created from the previous phase. The direction of flow of the data is always forward because it always flows from input layer to output layer.

6.2.4 Network Initialization

This phase stipulates the accessible weights using an equation of weighting on every connection: $w(t+1) = w(t) + \eta\delta w(t)$. Both the weights w(t+1) and t+1 are equivalent as the learning rate times measured change in the weight.

6.2.5 Training Process

To get the desired output, for the purpose of input dealing, training the network is must. For network training, several kinds of learning algorithms are used in the literature. The kinds may categorize into two algorithms, i.e., supervised and unsupervised. In supervised algorithms, the network training is done by provision of training examples that include the matching of patterns (input to output). In unsupervised learning algorithms, the training of the network is done first then features are gained from internal data. Some reinforcement algorithms are also used that combine both supervised and unsupervised techniques, wherein the weights for the network are raised or reduced for honor or penalty [173]. A popular method for training artificial neural network is the back-propagation algorithm [174]. As a supervised learning algorithm it is beneficial for feed-forward networks. It is possible to implement the back-propagation algorithm in two phases, i.e., forward and backward pass. The addition of input to the neural network in the forward pass and

is propagated to measure the output through all neurons in the layers. The error determination for each output neuron is done in the last step. The concealed weights among neurons are modified in the backward pass. The hidden layer errors for neurons are measured and returned to the neurons. In this study, by finding convolution of inputs with their corresponding weights, the net inputs are determined. The outputs are defined by applying the net output activation function. To classify the succession among the activation value (zero and one) logistic function is being utilized. The activation value is assumed to be the same as the input layer's output. The anticipated output is determined in the way that: comparing all the with the values that were saved, the desired output value becomes '1' in the case of equality, and it stays as '0' otherwise (Figure 6.6)

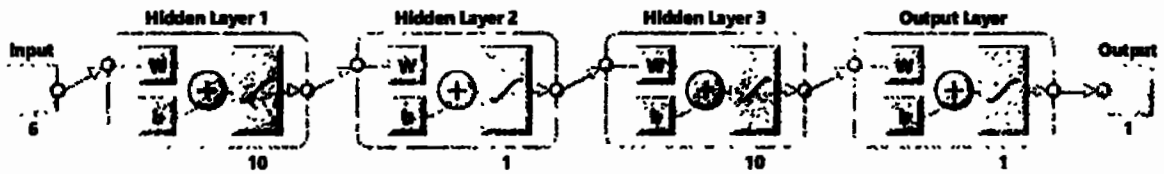

Figure 6.6: Structure of ANN

The prediction method for errors is carried out as follows:

$$O_{er} = D_{op} - N_{op} \tag{6.1}$$

where 0_er is the error of the output layer, D_op represents desired output, and N_op is the network output.

Backward pass input layer errors are calculated as:

$$I_{er} = I_w - O_{er} \tag{6.2}$$

where I_er represents input layer, I_w is the weight of the input layer and O_er is the output layer error. Input and hidden layers weights are modify accordingly. Calculated errors are measured against the preset error value that changes the algorithm of the back propagation.

The Mean Square Error (MSE) function for this purpose is used as follows:

$$MSE = \frac{(D_{op} - N_{op}^{'})^2}{2} \tag{6.3}$$

where N_op is the network output and D_op is the desired output.The algorithm stops if the current error exceeds the maximum acceptable value, or if the full training is achieved by the network and the error value is zero. The MSE for best validation performance is shown in the figure (Figure 6.7)

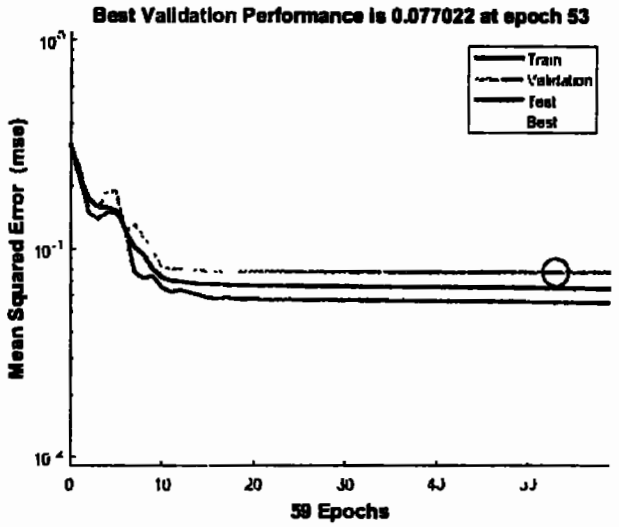

Figure 6.7: Mean Square Error

6.2.6 Recognition Process

After finalizing the training process, the network becomes ready for the process of behavior recognition. For calculating the final values of the output layer, maximum percentage value of same layer is extracted. For instance, if the percentage is 15, then this indicates that the behavior while drawing the pattern is original at 15% and not identical at 85%.

6.3 Experimental Results

To assess the viability of the proposed system, a thorough user study was conducted. Data from 25 volunteers were collected. ANN classifier is trained to evaluate predictive output using the test data set.

30 students from our university (12 females and 16 males) voluntarily participate in this study. Presentation with animations was given to them, to explain the concept of the proposed authentication system. Participants created their account after choosing their required credentials of registration phase. They were asked to get login into their smartphones using the proposed system. False rejec-

tion rate (FRR) and false accept rate (FAR) are the key performance parameters for mobile-based behavior authentication systems. FRR recognizes and denies mobile phone access to authorized users as unauthorized users (equation 6.4), and FAR treats unauthorized users as authorized users (equation 6.5). This chapter analyses the proposed authentication system for both efficiency and accuracy. Symbols in the following equations are mentioned in table 6.3

Table 6.3: Symbols of Equations

Equation	Symbol
No. of authorized user access denied	AuD
No.of login attempts by authorized users	LaA
No.of unauthorized user access approvals	UuA
No.of login attempts by unauthorized users	LaU
True positive	Tp
True negative	Tn
Total Instances	Ti

$$FRR = \frac{AuD}{LaA} \tag{6.4}$$

$$FAR = \frac{UuA}{LaU} \tag{6.5}$$

The obtained results show the FAR 4.36 and FRR 5.03. Accuracy of classification, that is the ratio of correctly classified instances (equation 6.6).

$$classification_accuracy = \frac{T_p + T_n}{T_i} \tag{6.6}$$

The accuracy in our example is 0.75% and the error rate is 0.25%, so a high percentage of instances can be correctly labelled by the model.

6.4 Comparative analysis

In this section the proposed authentication system has been evaluated against different known attacks. Furthermore, a comparative analysis of the proposed authentication scheme has been presented with the existing authentication schemes.

6.4.1 Shoulder Surfing & Smudge Attacks

Shoulder surfing being a real threat to authentication systems is of two types. First, weak shoulder surfing in which an attacker directly observes the authentication mechanism, and second, strong shoulder surfing in which attacker uses any hardware device i.e. recording camera [13]. In the proposed authentication scheme by using small arithmetic operations i.e. addition and subtraction, user draws a unique pattern on every login session and thus make it difficult for the shoulder surfer to catch. If the shoulder surfers try to authenticate, a new P-code indicator will be shown at the screen, and he will not be able to process the Pass-code without the R-code digits. If the attacker captures the user's pattern via the camera, the P-code indicator will be different in the next login session. Participants were divided into two groups, 16 of them acted as the attackers (shoulder surfer and smudge attacks) and 14 acted as users. The attackers were well briefed about the two attacks. In the video or by looking over the user's back, the attackers need to notice the user's P-code indicator and hand movement. When drawing the authentication pattern to conduct skilled attacks, the attackers can watch the videos as much as possible to practice the user's behavior. A total of 1650 samples were used for test set. An attacker first have to assume the values of R-code to process with server given P-code indicator values. Even if he knows the values and know what pattern should be drawn, he has to draw the resultant pattern according to the behavior of the user. The results showed that when an attacker draws the PPA pattern, in sitting posture the success rate of attack was 3% while walking, the shoulder surfing and smudge attack is not possible.

6.4.2 Comparison Analysis

Table 6.4 presents the proposed work's comparison with the projects using ANN in different ways to provide security for smartphones' authentication. The findings describe their proposed work. This article proposed a method that provides the security in the registration phase and a multi-factor security in the authentication phase. [114] uses brain signal which is limited to the proposed framework, however our proposed scheme uses simple mathematical calculation that to draw the required login pattern. [116] does not reduce the password complexity. The proposed authentication scheme combines the behavior authentication and "something you process" authentication factors in a graphical box having two lines of defense, i.e., a unique pattern indicator, which shows a different value to the user at every login attempt to construct the pattern, and a pattern checker that verifies the pattern correctly.

Table 6.4: Related work comparison of PPA

References	Algorithm	Findings	Constraint
[114]	ANFIS	The ANFIS produces the lowest error rate and cosine similarity	Authentication by brain signal across the network is limited to the proposed framework
[115]	ANN-LMNN	In both optimization and authentication, ANN-LMNN provides better efficiency	The ANN has the chance of being stuck in the local minima
[116]	ANN-BPNN	The ANN gives better results than other classifiers	The proposed research could not alleviate the password complexity of the system's protection and usability.
[108]	ConvNe	ConvNet has the highest accuracy in predicting the behavior's action of the user than the compared algorithms.	To get the many-features-hierarchy, the CovNet contains too many layers
Proposed PPA scheme	ANN	Two factor authentications using ANN for behavior features	User joins only two nodes for authentication

6.5 PPA with Support Vector Machine

In the high-dimensional feature space created from the initial sensor values, the Support Vector Machine (SVM) can identify more detailed relationships within the data [175]. The SVM classifier was trained using the above attributes acquired from various users as training data, and the collected data was labelled as valid users (1). After the algorithm has been taught, it can tell whether a valid user or another person attempted to log in. The LIBSVM [176] implementation of SVM was utilised to support the estimation of probability. The algorithm will determine whether or not the drawn pattern was created by an authorized user. The positive samples, which consist of patterns from a genuine user, and the negative samples, which consist of patterns from all other users, are the two classes required to learn the SVM.

confusion matrix figure 6.8 show the obtained true positive and true negative values, i.e., registered users were correctly recognized as valid users, and 28 registered users were falsely recognized as invalid users. 9 unregistered users were wrongly verified as registered users and 244 unregistered were truly verified as non authentic users. The obtained results show the value of FAR 0.10 and FRR 0.02 and an AUC of 99% as shown in figure 6.9.

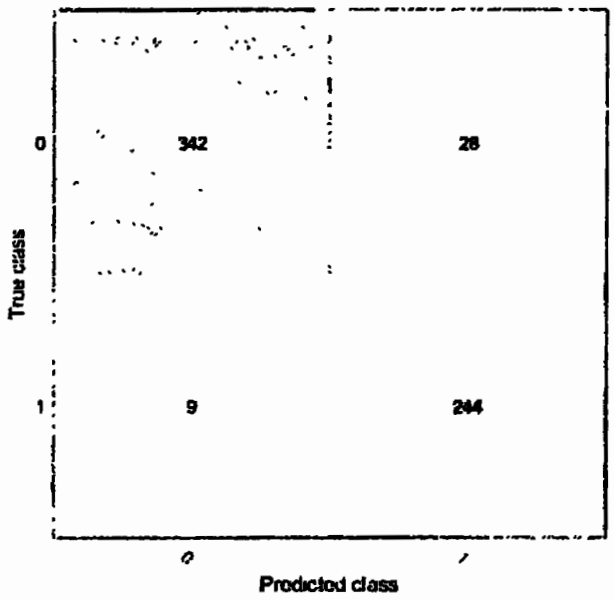

Figure 6.8: Confusion matrix of PPA with SVM classifier

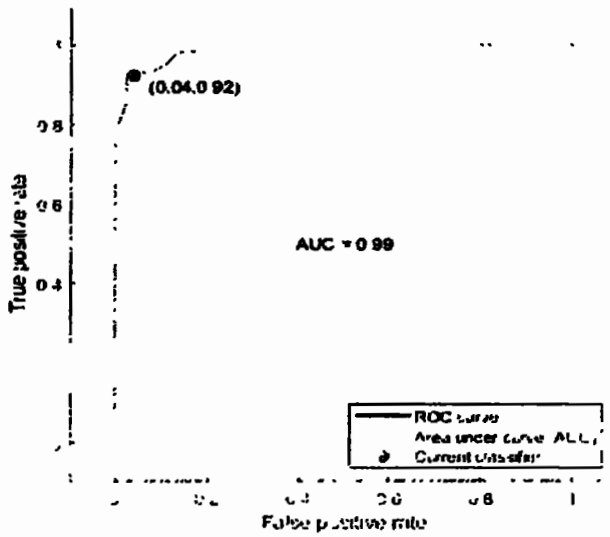

Figure 6.9: Accuracy of PPA with SVM classifier

6.6 Summary

With the growing tendency of network services and applications, users can access such applications through various IoT gadgets. Therefore, as to ensure users digital property, there is need of validation each time they attempt to reach their personal data or accounts. Textual passwords or PIN methods are commonly used by most of the users to be authenticated. People use small passwords because complex passwords are not easy to remember or they even use one password for various accounts. Thus, attackers can easily guess the passwords. Some of those attacks do not require any special technique or software, e.g., shoulder surfing and smudge attacks, to steal information. Graphical passwords are more secure than the textual ones and are difficult to crack. The graphical authentication system is more user friendly and removes the difficulty of remembering complex passwords. Cracking the graphical passwords through guessing is so challenging for the attacker, dictionary or brute force attacks. The contribution of the proposed authentication scheme is that it combines the behavior authentication and "something you process" authentication factors in a graphical box. Furthermore, it has a two levels of defense system, i.e., a unique pattern indicator, which shows a different value to the user at every login attempt, and a pattern checker that verifies the pattern correctly. In this proposed multi-factor behaviour authentication technique, the user's drawn pattern is verified to see if it is accurate or not before the accuracy of the pattern is determined using the user's login behavioural attributes. Later, it authenticates users on the basis of touch behavior features. For authentication purpose, the sequence of position is not considered in the proposed method. The future work can include physiological and moving sensors for user identification in the IoT environment.

Chapter 7

Instruction Based Handwritten Authentication using Machine Learning

User authentication is important in the case of the Internet of Things (IoT) to ensure the security of attached appliances and to customize the service. The strong sensing capabilities of IoT devices allow continuous and implicit authentication based on behavioral biometrics, containing smartphones, wearables, robots, and independent automobiles. Schemes based on passwords/PINs/patterns are at risk to shoulder surfing and smudge attacks. In addition, for users to enter regularly, passwords/PINs/patterns are inconvenient. Using something you process authentication factor, this thesis presents Machine Learning Instruction Based Handwritten Authentication (IBAM). At every login attempt, the server provides a user two numbers along with a mathematical operator to be processed by the user with the numbers given at the time of registration. Instead of typing it on a keypad,PIN codes is requested to be drawn by the user on the touch screen. Consequently, using behavioral biometrics with a new processed password at every login attempt, as an additional authentication factor further away than the PIN's concealment, IBAM provides ::or security. For handwritten digits identification, this thesis present a method based on CNN (convolutional Neural Network). The implant neural network is being trained in this approach to recognize similarities and patterns between various samples of handwriting. Experimental results show that the situation in which hacker is aware of the PIN by shoulder surfing, IBAM achieves an equal error rate of 4.6%.

Within our lives, electronic appliances are popular. They are able to connect via both the Internet of Things (IoT) and the public network. Mobile appliances come to be an essential tool for nearly all

the individuals today. The widespread adoption of IoT devices in the market assembles it significantly necessary for user authentication to ensure that users have an adequate freedom to approach IoT appliances and to prevent the catastrophic damage because of a single attack that occurs at unsafe locations [177]. Normally users uses pattern or Personal Identification Numbers (PIN) lock system to unlock the device. The single factor PIN and One-Time Passwords (OTP) have historically been the two most dominant user authentication approaches on mobile devices [178]. In PIN authentication technique user memorize their secret PIN codes to unlock their devices. OTP-based systems prevent users from memorising the PIN codes, because on every login attempt, the system is responsible for selecting and giving the user with a new password, by transmitting the content to personalized mobile appliances or particular tokens. These authentication systems are often vulnerable to shoulder surfing attack i.e. imposter can peak from the user shoulder to get the PIN/pattern or use external device like camera to record the finger movements of the user while unlocking the device. PIN/passwords are also susceptible to smudge attacks, i.e. the imposter can guess the password or unlock pattern of the user's device by examining the smudge left on the device screen[179]. Researchers showed that they conceivably recreate a PIN out of minimum ranked video (recorded from a distance by a smartphone or Google Glass camera) through capturing movement of the hand or fingertip in the procedure of entrance of the PIN with a success rate of till 90% [180].

With the combination of the maximum security and the ease of use, biometric authentication schemes can respond with these challenges [104]. Biometric authentication has normally two types, i.e. physical and behavioural. Physical biometrics are based on user-inherent physiological features for example palmprint, iris, face and finger prints, while behavioural biometrics are related to non-physiological features that can be replicated in a particular way by a user. for example voice, keystroke, and handwriting. It is difficult to adapt physical biometrics while behavioral biometrics are changeable [181]. With the exponential growth of machine learning techniques, the challenges of biometric authentication using machine learning have been addressed by an growing amount of study.

This chapter has proposed a multi-dimensional behaviour pattern lock system. First, the user must compute the PIN code values, utilizing the "something you process" feature for authentication. Something you process factor also known as formula base authentication technique provides secure authentication against shoulder surfing attack, as a user on every login, enters a different password. Operation code authentication [44] uses this factor of authentication to avoid shoulder surfing and smudge attacks. Every user on each login will get random values from the server, the user

processes the given values in a formula and calculates his password. Secondly, he will write the digits of the PIN codes and will get authentication barely in case the digits of the PIN codes and the user's touch dynamics features are similar to saving features in the system. This article suggests Convolutional Neural Network (CNN) in a finger-drawn PIN code authentication scheme for the task of digit recognition that is carried out on solo handwritten digits obtained by a touchscreen mobile phone. CNN is layered, with a single layer (input and output), several hidden layers or not. ANN would be spotted to enhance the security of touch screen applications for mobile phones [120]. The artificial neural network pattern recognition approach has been steadily replacing the conventional method of pattern recognition in recent years. Pattern recognition has become the latest, more mature technology after years of research and development and has been commonly implemented in computer vision, voice recognition, remote sensing image recognition, fingerprint recognition, handwritten character recognition, face recognition, etc.

Instructional handwritten authentication based on machine learning (IBAM) was installed on the smartphone of users who were asked to use this application for ten days. User has to process the digits of his/her PIN codes by applying either addition or subtraction operation between Passcode (PC) i.e. numbers given by the server at the time of authentication and Registration code (RC) the numbers which he gave at the time of registration. By applying the arithmetic operation, a new PIN will be generated at every login attempt. The authentication method recognises the IBAM PIN digits and tests the similarities between the handwriting of the input and the handwriting of the recorded users saved in the database. In the case of the recorded user, access will be granted.

The main contribution of this chapter in this thesis are:

- This chapter review and analyse the benefits and drawbacks of recent touch biometrics research for mobile authentication.
- Machine learning instruction base authentication (IBAM) system is proposed in this article, that allow user to enter a new PIN every time when he/she login

  While typing PIN codes on touch screens, a collection of effective features that capture behavioural information.
- A complete data set consisting 2000 training samples from 50 users was gathered and IBAM's execution on this data set was evaluated.

7.1 IBAM

In this thesis we have proposed an Instruction based behavioural authentication, using the concept of something you process authentication factor with behavioural biometric to ensure secure authentication. IBAM has two phases, registration and authentication.

7.1.1 Registration Phase

The registration phase of this proposed scheme is an individualized process because the user will complete the registration process without having to understand the logic. In the registration phase, a user has to choose username and two numbers between 0 to 9. These user-selected numbers will be referred to as the Registration code (R-code). Let us suppose that the username is ALI and the R-code is 1,4. Fig. 7.1 shows the flow chart for this phase.

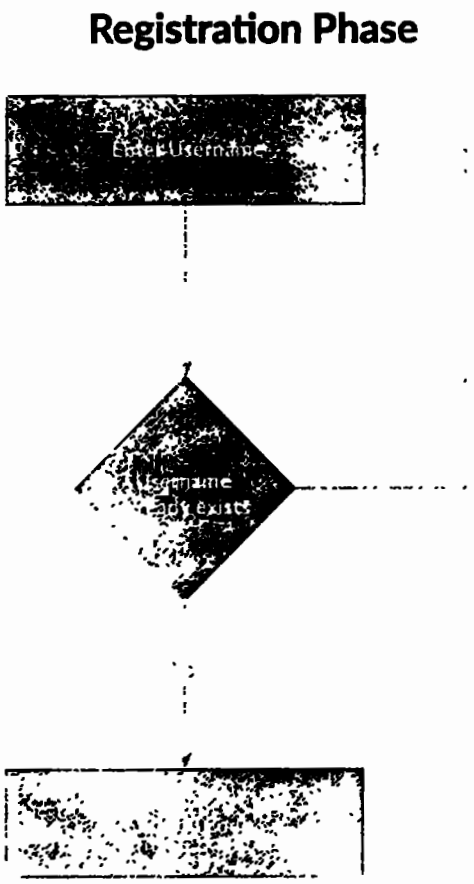

Figure 7.1: Flow chart of Registration phase

7.1.2 Authentication Phase

In this phase, the user has to enter his/her username. The process code generator (PCG) will give two a number i.e. Process code one (PC) along with a mathematical symbol of either addition or subtraction. The user will perform the mathematical operations between the first digit of his selected R-code and information given by the Process code generator and will write the first resultant PIN digit on the screen. The authentication server will check two things, i.e. the PIN digit entered by the user is correct or not, and the behavioural features of the user while writing the first PIN digit. If the authentication server founds the user's written digit correct and behavioural patterns matched with the saved pattern of the users then the server will move to the next step of authentication, if any one of them fails, PCG will give PC1 and mathematical symbol again. PCG will give the second PC digit along with a mathematical operation, the user will operate with his second R-code digit and will write the second PIN digit on the screen. The server will give such P-codes to the user whose mathematical operation results lies between 1 to 9. Fig. 7.2 shows the flow diagram of this phase.

7.1.2.1 Working Example

Let us suppose that Ali is the username and his R-codes are 3 and 4. When he tries to login into the device, the server will give him the first P-code number with either addition or subtraction operation. Let us suppose that the instruction from the server is to add 2, thus he has to add 3 (his first R-code digit) with 2 (first P-code digit), the result is 5, and this will become his first PIN code digit. The user will write 5 on the touch screen of his device. If the resultant PIN code is correct and the behavioral features of the user while typing the digit 5, match with the features in the local database, then the user will move to the next step of the authentication process, otherwise the authentication process with stop. Let us suppose that the next instruction from the server is to subtract 1, thus he has to subtract 4 (his second R-code digit) with 1 (second P-code digit), the result is 3, and this will become his second PIN code digit. The user will write 5 on the touch screen of his device (Fig. 7.3).

Table 7.1 shows the different notations of the proposed algorithm used in the pseudo-code.

The pseudo-code of the proposed IBAM scheme has been shown in Algorithm 1.

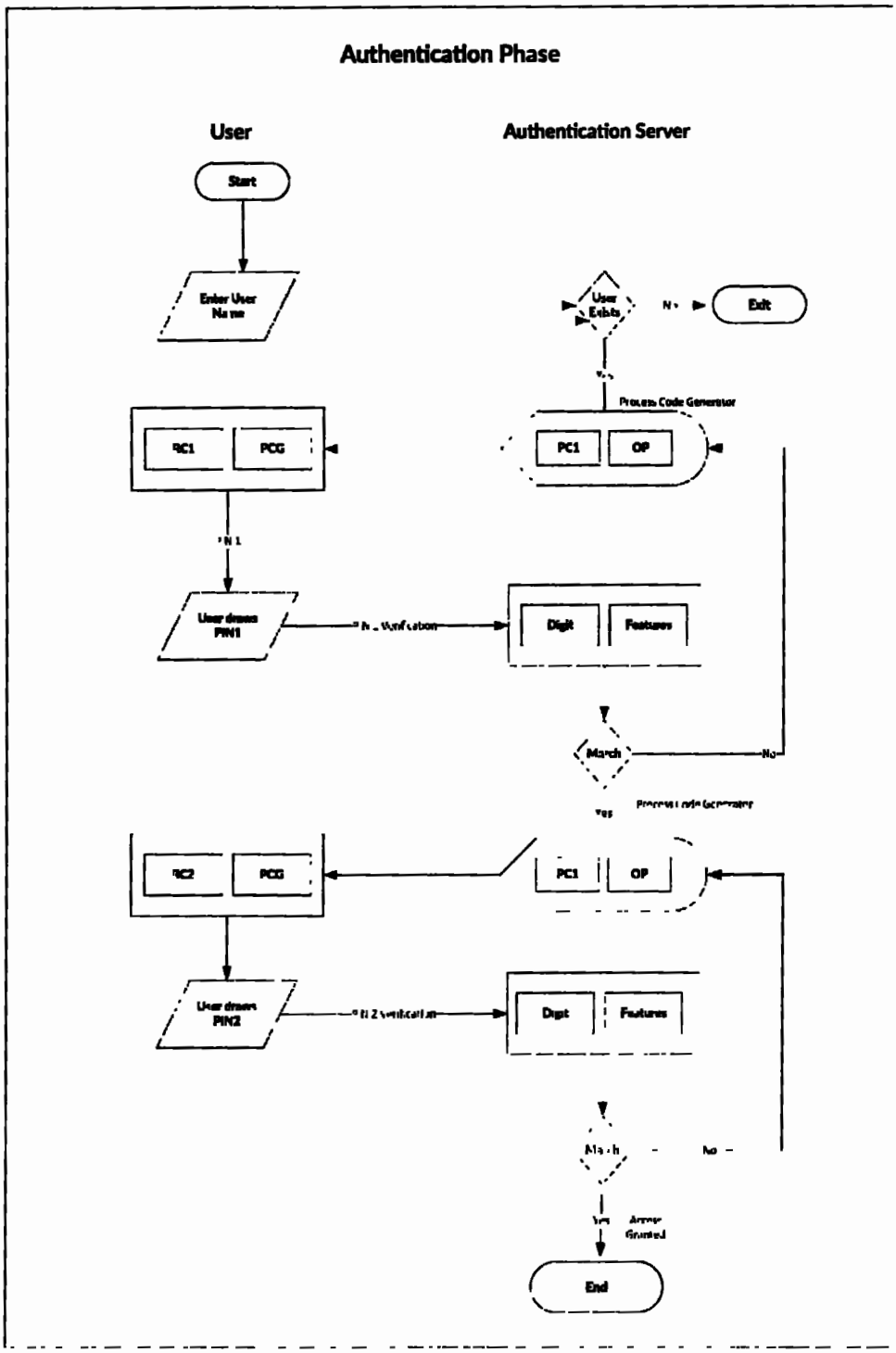

Figure 7.2: Flow chart of Authentication phase

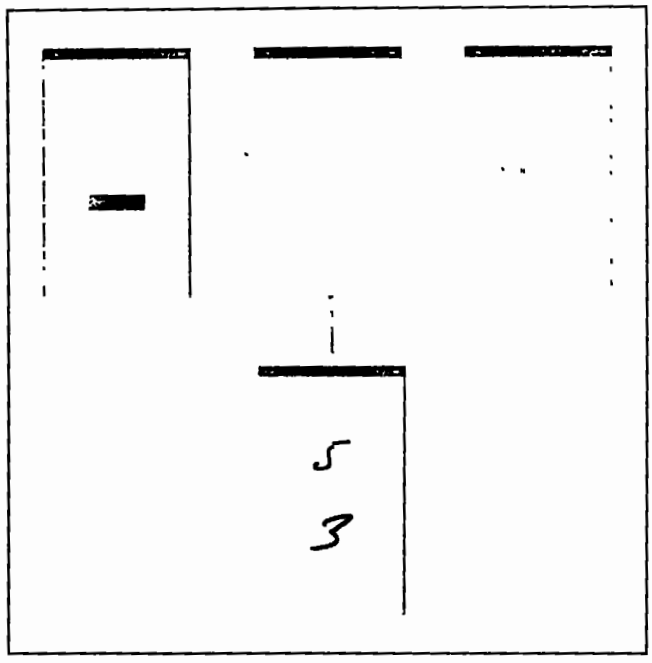

Figure 7.3: IBAM: Login and authentication phase

7.1.3 Data Collection and Training

There are two types of pattern identification and verification for human writing digits/alphabets on the touch screen. The first one is Dynamic real-time verification: It is suitable for the identification of patterns on mobile devices. The other one is Offline static verification: It is suitable for characters, digits, and patterns on paper. In this research, we have adopted a dynamic real-time verification approach as it is well suited for touchscreen devices. By utilizing the IBAM authentication method users were asked to unlock the screens of their mobile appliances after the installation of the IBAM. There are several methods for classifying and identifying handwritten digits. The availability of three sensors along with a touchscreen in the latest mobile phones is considered by IBAM: the gyroscope, the magnetometer, and the accelerometer, which provide various levels of knowledge on the user's behavior. Details about the mobile phone sensors are shown in Table 7.2.

An Android application was built and the user was asked to draw digits from 0-9 in two different methods. In the first method, the user will write 0 to 9 to 100 times on his touch screen. And in the second method user will write every digit i.e. from 0 till 9, 100 times. The user trained the CNN classifier on the digits 0-9 using the above methods. A CSV file was created which gave the labels to the digits according to the values obtained from the sensors mentioned in Table 7.2.

Table 7.1: Notations used in pseudo code

Notations used in Pseudo code	Notation description
User Name	U_n
Registration Code 1	R_{c_1}
Registration Code 2	R_{c_2}
Random Number 1	R_{n_1}
Random Number 2	R_{n_2}
Process Code 1	P_{c_1}
Process Code 2	P_{c_2}
Mathematical Operation(addition or subtraction)	OP
Pin Code 1	P_1
Pin Code 2	P_2

Table 7.2: Sensors embedded in mobile phones

Sensor	Sensor Description
Magnetometer	Computes the axes(x,y,z) regarding system geomagnetic sector
Accelerometer	Computes the force of acceleration along with the force of gravity
Gyroscope	Computes the rotation of device along the axes (x,y,z) with mobile phone's movements(roll, pitch and yaw)
Pressure Sensor	Measure the pressure placed on the screen

For writer verification, the CNN classifier was trained based on features described in Table 7.3 from different users. Non-linearity, uniformity of analysis and design and input-output mapping are some of the capabilities of CNN. Multi-layer perceptrons and radial basic functions are the most commonly used CNN architectures for pattern recognition systems. The input layer is used to process sensor data to extract low-level features. Hidden layers perform further processing to extract high-level features. The output layer makes a decision based on the hidden layer output. Latest mobile phones have various sensors that are built-in from these the sensor(s) were chosen that precisely mirror the user's behavioral characteristics while drawing the IBAM PIN digit. IBAM considers the available three sensors along with the touchscreen in the latest mobile phones: the gyroscope, the magnetometer, and the accelerometer, which provide various levels of knowledge on the user's behavior.

The first type of data is collected through a touch screen that includes the pressure (pressure), finger location coordinate X, Y (fingerx, finger), timestamp (timestamp) and the contact area height(size).

The data that was gathered is provided as training data and categorized as valid users (1). After the training of the algorithm, it checks whether an authorized user or someone else has attempted

Algorithm 1 IBAM: Instruction Based Handwritten Authentication

Input: U_n, R_{c_1}, R_{c_2}
Server Input: OP
Output: P_1, P_2

1: Registration process (Choosing of U_n, R_{c_1}, R_{c_2})
2: Login Process (Enter U_n)
3: **if** U_n = True **then**
4: $R_{n_1} \leftarrow P_{c_1}$
5: $P_1 \leftarrow R_{c_1}$ OP R_{n_1}
6: **if** P_1 = True **then**
7: $R_{n_2} \leftarrow P_{c_2}$
8: $P_1 \leftarrow R_{c_1}$ OP R_{n_1}
9: **if** P_2 = True **then**
10: ACCESS GRANTED
11: **end if**
12: **end if**
13: **end if**

to Login.

Table 7.3: Extracted features of sensors and touch events along with symbols

Symbol	Name of Feature
T_{dr}	The time between touch down and touch release
T_p	Average force of the touch
S_{tp}	Standard deviation of force of touch
M_p	Maximum force of the touch
M_{np}	Minimum force of the touch
S_s	Finger's sliding speed between points
S_a	Finger's sliding angle between points
N_s	Number of touch events of each segment
$T_{..}$	The maximum limit interval between two moving events for making a moving pattern.

7.1.4 Model Training Session

For this research, a data set of handwritten digits has been developed. 50 students of undergraduate semesters were recruited for the training sessions. We collected 40 samples from each student, i.e. 2000 samples in total. The average time taken by each individual in writing 10 digits was 20 seconds.

7.2 Results and Analysis

For our research, 30 volunteers (18 males and 12 females) were between 20 and 30 years of age and each Android phone holder is enlisted as a user. The users were introduced to the research at the beginning with the help of an animated presentation and app downloading on their phones was demanded by them. Every user was asked to unlock his/her device by using the IBAM app for 10 days. The user draws his/her two digits PIN code by applying mathematical operation on his or her selected R-codes and server-given P-code digit. Data was obtained without supervision over 10 consecutive days. Overall 3203 PINs drawn with fingers, as well as 150 samples of training (five for each user) and 3103 samples of login, were obtained, along with 599 samples of unseen PINs drawn with the finger. Unseen PINs drawn with a finger can boost durability in opposition to shoulder surfers, besides this may also change the precision and convenience of authentication. In the second part of the experiment, 25 participants were invited to be the attackers for the selection of falsification samples. The shoulder surfer participants were allowed to examine the smudge left on the device of the legitimate user. Then the drawing of the PIN (five times) was demanded by each attacker. Every PIN was drawn by them in a different manner as the originally drawn Pins by the users were not recognized by attackers. On average, there were 105 samples of attacks regarding every user, overall, 2180 samples were obtained regarding PIN attacks.

We have applied classification using CNN for the detection of numbers. Each number has pixels in the form of dimensions. We trained the samples using CNN and then test the samples. Convolutional Neural Networks are a particular sort of multi-layer neural network created to identify visual patterns effectively from images obtained with little preprocessing. Almost all CNN architectures adhere to the same fundamental design concepts, which include applying convolutional layers to the input one at a time, frequently downsampling the spatial dimensions (using Max pooling), and increasing the number of feature maps. In addition, completely connected layers, activation functions, and loss functions exist (e.g., cross entropy or softmax). Convolutional layers, pooling layers, and fully linked layers, however, are the most crucial CNN operations. So, before outlining our suggested model, let's quickly introduce these layers.

The first layer that can extract features from images is the convolutional layer (figure 7.4). Convolution enables us to maintain the relationship between various components of a picture because pixels are only related to their immediate neighbours and close neighbours. Convolution is a technique for reducing the size of an image without sacrificing the relationship between its pixels. The complexity is reduced by 64% when convolution is applied to a 5×5 image using a 3×3 filter

with a 1 × 1 stride (1-pixel shift at each step).

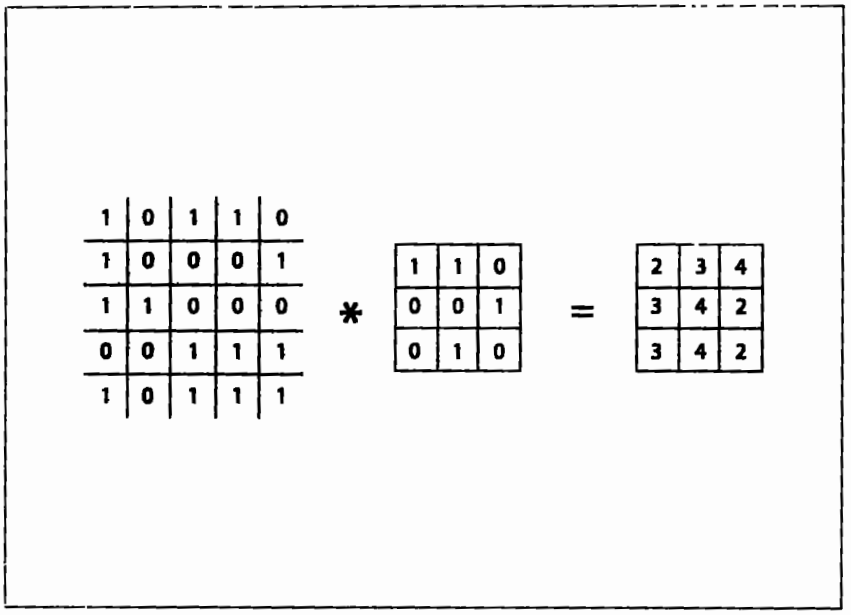

Figure 7.4: Convolution operation

In order to condense the spatial size of the feature maps in a CNN, pooling layers are frequently added after each convolution layer. The overfitting issue is also helped by pooling layers. By choosing the maximum, average, or total values inside these pixels, we choose a pooling size to reduce the number of parameters. One of the most popular pooling strategies, Max Pooling, can be demonstrated as follows figure 7.5:

Any architecture where the relationships and effects of each parameter on the labels are determined by linking them together has a fully connected network. We can ultimately build a fully connected network to identify the images since convolution and pooling layers reduce time-space complexity.

The architecture of our suggested CNN model is shown in figure 7.6. We must first perform some preliminary processing on the images, such as shrinking them and levelling their pixel values. Data is prepared to be provided to the model after the required pre-processing. Convolutional layer with ReLu (Rectified Linear Unit) activation function makes up Layer 1. The input for this layer is a pre-processed image with a size of $n \times n$ =28 × 28. Layer 2 is the the maximum pooling layer. Each feature map independently does max pooling, giving us the same amount of feature maps as the previous layer. Layer 3 is the second convolutional layer with the ReLu activation function i.. layer three. Layer 4 is the second max pooling layer. Layer-5 is the third convolutional layer without ReLu activation function. The fully connected layer is Layer 6. This layer produces a one-

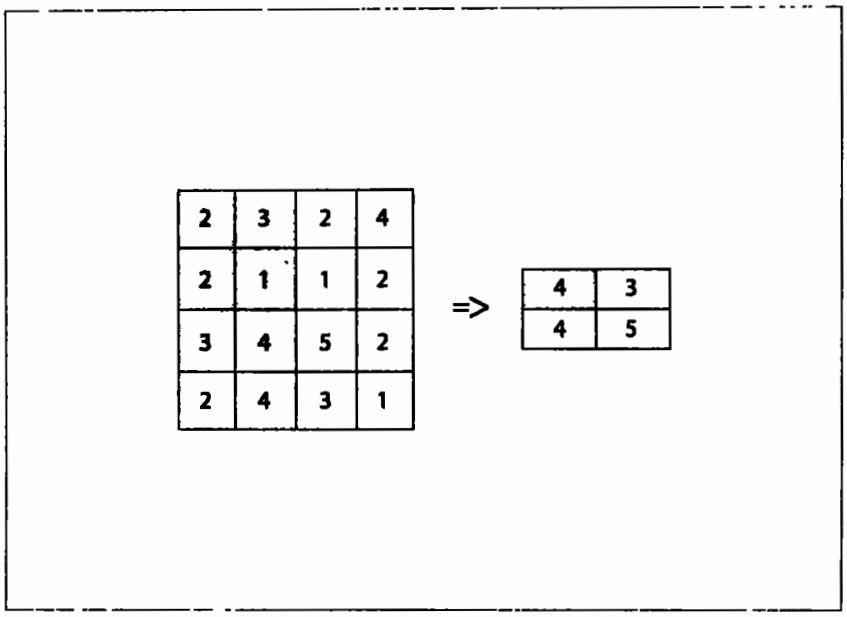

Figure 7.5: Max pooling Operation

dimensional vector of size 256 from a 64-dimensional input vector. It has the ability to activate ReLu. The final layer of the network is Layer 7. It has complete connectivity as well. In general, the convolution / fully linked layers carry out transformations that depend on both the parameters and the activations in the input volume (the weights and biases of the neurons). The ReLu/pooling layers, on the other hand, will implement a fixed function. To ensure that the class scores for each image are consistent with the labels in the training set, the parameters in the convolutional / fully connected layers will be trained using the stochastic gradient descent approach. In order to categorise the digits in the test data, the algorithm will prepare the trained model. The digits seen in the images can be categorized from class 0 to 9.

Similarly, we have recognized the users using CNN. All the digit samples are categorized w.r.t. each user. Digits are recognized correctly using CNN features and achieve an overall accuracy of 99%, which means that a user will be denied twice in every 100 trials. Figure 7.7 shows the training loss and training accuracy predicted by the proposed model. Loss indicates how well the model is fitting the training data.

The training accuracy is computed using TP+TN/ TP+TN+FP+FN and in our context, it represents the number of images that are correctly classified among all of the test images.

We have evaluated the digit recognition table 7.4 using the following accuracy metrics.

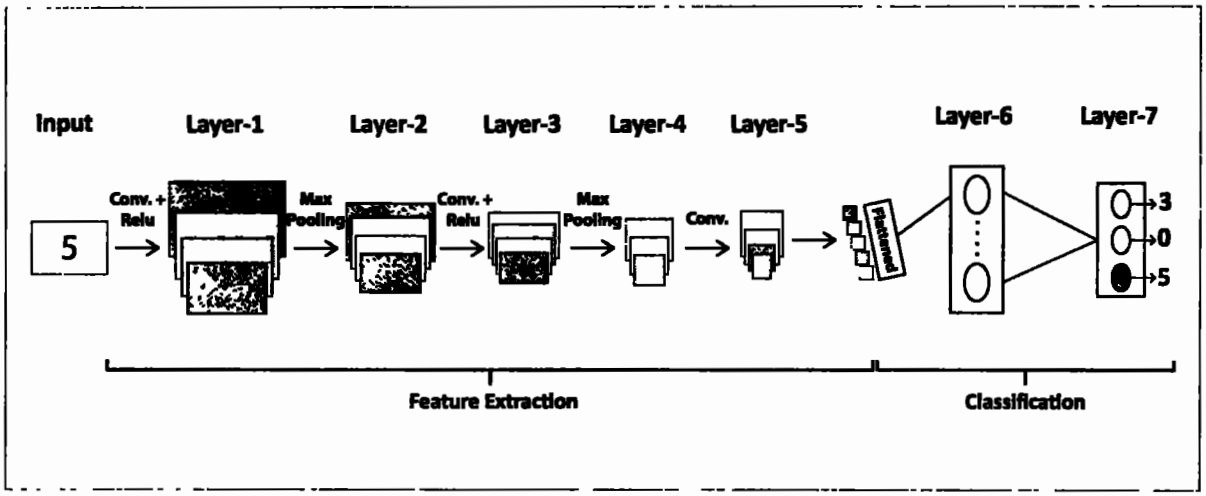

Figure 7.6: CNN architecture

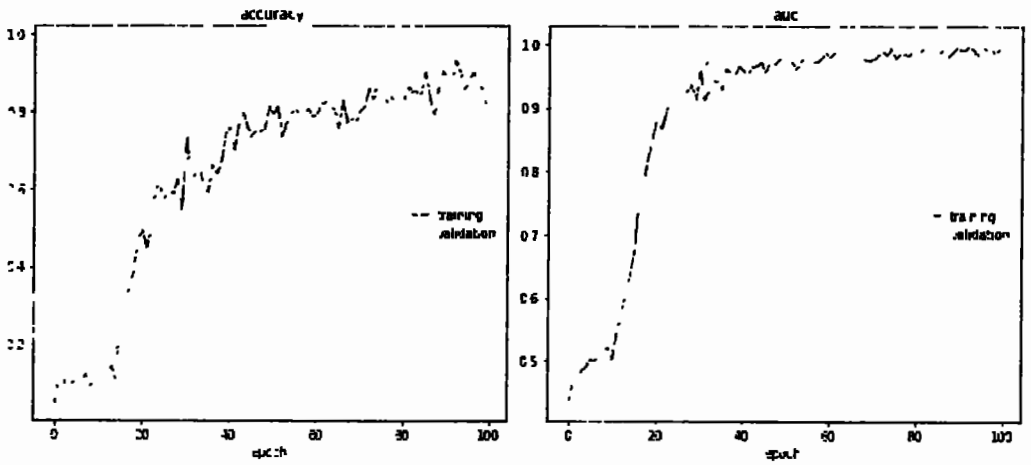

Figure 7.7: Precision and recall of digit recognition

Precision: It is defined as TP/TP+FP that represents the ability of the classifier to avoid false positives. Since we have a multi-class classification problem.

Recall: It is defined as TP/ TP+FN and represents the ability of the classifier to avoid false negatives.

Table 7.4: Performance Parameters

Accuracy	RecallPrecision	Sensitivity
0.99	0.910.95	0.92

7.3 PPA with MNIST Dataset

The MNIST data set [182] is also used as historical handwritten digital data for this proposed scheme. A fairly well-known data set in the field of machine learning is the MNIST data set (figure 7.8. There are two sections to its data set: a training set and a test set: each piece of data in the training set and test set contains a handwritten digital picture (displayed as a 28×28 pixel gray scale image) and its corresponding label (displayed as 0-9) label. The training set contains 60000 pieces of data and the test set contains 10,000 pieces of data.

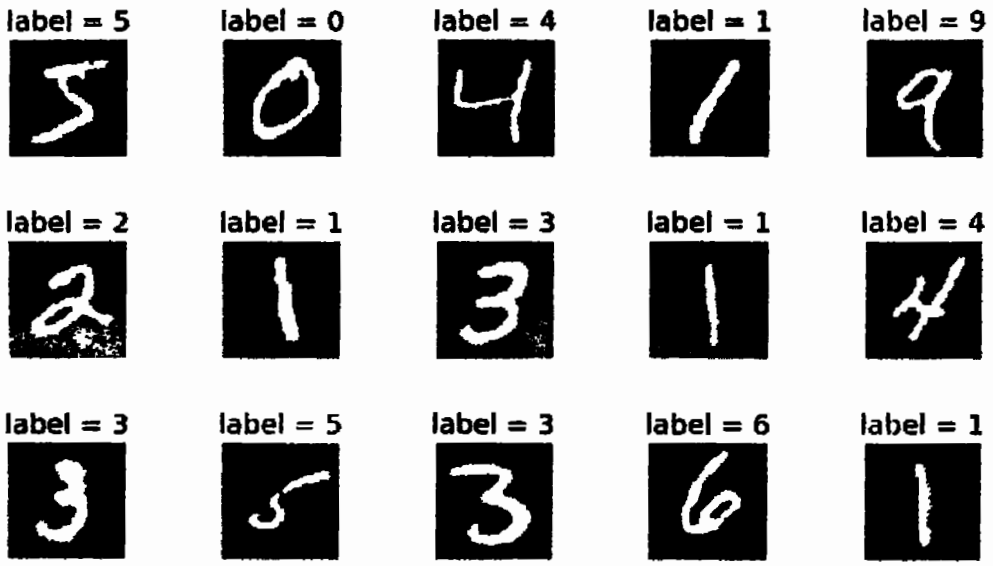

Figure 7.8: Precision and recall of digit recognition

In some ways, CNNs are similar to classic artificial neural networks (ANNs) in that they are made up of Self Optimizing Neurons, each of which processes input to produce a scalar product with a non-linear function. CNNs are regularised variations of multilayer perceptrons, which typically refer to fully connected networks in which each neuron in one layer is connected to all neurons in the next layer, and whose final layer contains loss functions associated with the classes while the network as a whole still expresses a single perceptual score function (the weight).

Using the back-propagation algorithm LeNet-5 convolutional network, which may be utilised for identifying significantly changing patterns, we trained the CNN on the MNIST handwritten digital database. 28*28 neurons are used to build the input layer, which represents the size of images. Along with an output layer of 10 neurons that represents the various classes of handwriting images, the hidden layer comprises 100 neurons with sigmoid activation function. The accuracy plot in figure 7.9 is shown by the accuracy obtained. The x-axis is showing the epoch values and the y-axis is showing the accuracy values and area under curve values respectively. The accuracy of the model is 99.53%. Here is a graph of our CNN model's training set accuracy (represented by the blue curve) and test set accuracy (represented by the orange curve).

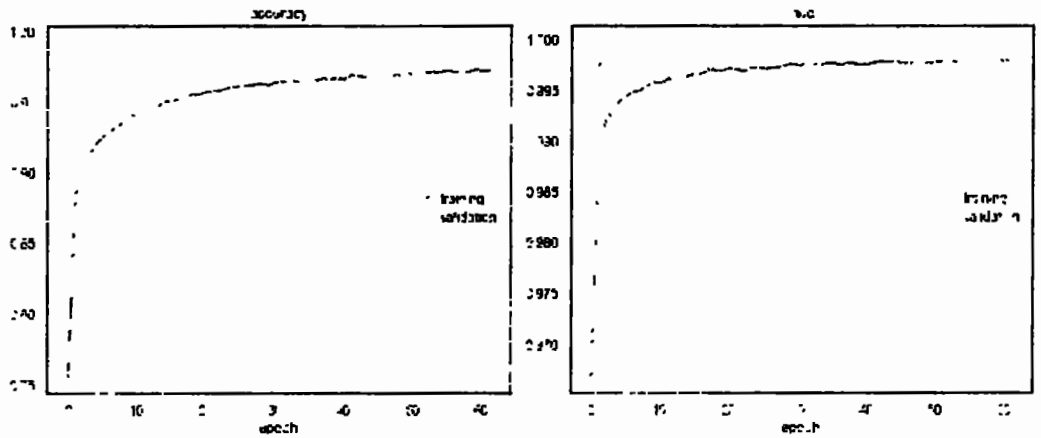

Figure 7.9: Precision and recall of digit recognition

IBAM is tested on two attacks, i.e. skilled and random attacks. A skilled attack corresponds to the person who knows the technique of the IBAM authentication system but still doesn't understand some substantial description regarding the drawing of the PIN. The IBAM EER under skilled attack is 13.6%, meaning that the device rejects 86.4% of attackers even though they know the PINs. This is promising because the success rate of the attack is 100% relative to standard PIN-based systems in schemes that are similar. Random attack corresponds to the attacker who records the IBAM

authentication system through a camera or peeks over the user's shoulder when he is entering the IBAM PIN digits. Under random attack, the IBAM EER is 3.6%, as the imposter doesn't know the technique and only observes the IBAM PIN digit, which changes at every login session.

IBAM verification performance is recorded concerning the Receiver Operating Characteristic (ROC) curve, True Positive Rates (TPR), False Positive Rates (FPR), False Negative Rates (FNR), and Equal Error Rate (EER), as per standard practice in a biometric-based device [183, 184]. The output regarding a binary classifier is captured by a ROC curve as its threshold is diverse. By organizing TPR corresponding to FPR at various limit values, it is derived. FNR is the percentage of valid samples regarding the login that the device refuses inaccurately. FPR, in comparison, is the percentage of samples wrongly accepted by impostors.

Fig. 7.10 shows the IBAM ROC curves under the two threats. IBAM's EER for attack regarding PIN is 3.6%, which indicates even though attackers know PINs, the framework denies them 96.4% of the time. This is promising because, for a similar case, the success rate regarding attacks is 100% as compared to a standard PIN-based device. EER is 13.6% under shoulder surfing attack. The increased success rate is unsurprising given the attackers' extensive awareness of the user's drawing actions in along with the PIN.

Despite this, the framework refused attackers 86.4% of the time. These findings suggest that IBAM can help to reduce the risk of shoulder surfing. Table 7.5 shows the ERR of IBAM under two attacks, i.e. the attacker knows the authentication process of IBAM and login to the system, and the attacker's shoulder surfed the PIN digits of the user.

Table 7.5: EER(%) of IBAM under two attacks

Attacks	EER
Familair with IBAM	3.6%
Shoulder Surfed	13.6%

Another essential aspect of checking the usability of a device is time-consuming. In the user study, the time parameters were collected to show the time of users while writing a 2-digit IBAM PIN for unlocking the system. For the 2-digit IBAM processed PIN, distribution is shown in Fig. 7.11, the average time consuming of processing and writing two IBAM PIN digits is 9.45 seconds. The increase in writing time will cause some intervals between each digit by observing the experiment process that the user would take some break after writing a digit. From the recent analysis, it is found that it would take an average of 4.7 seconds for the simple numeric PIN method to unlock the

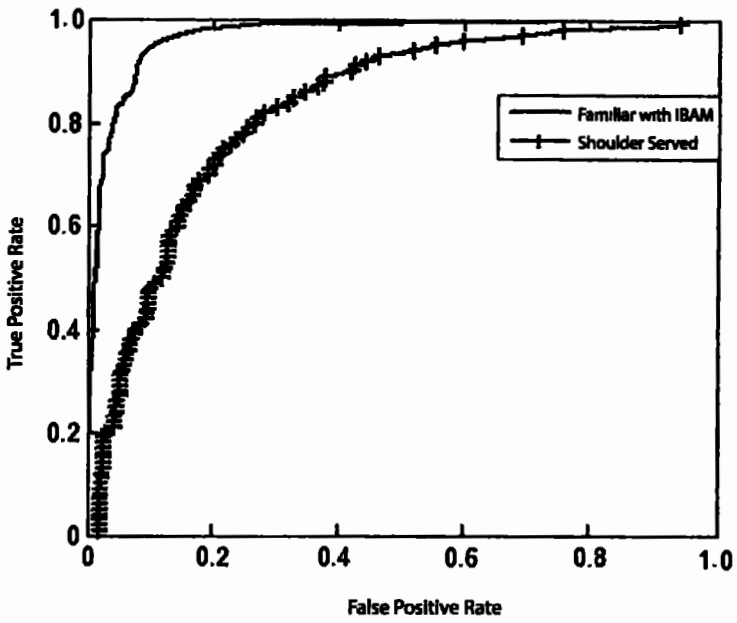

Figure 7.10: ROC curve of IBAM with two scenarios

device [185]. It is obvious that it will take a lot more time for our IBAM method than a simple PIN. We also question some of the participants to take their views about time-consuming to consider the effects on usability. The feedback mainly involves two opinions, firstly a small percentage of participants thought that this technique takes too much time on the writing behavior, and secondly most participants said that they did not find that when processing and writing the IBAM PIN digit it would take a lot of time as its very simple arithmetic operation.

IBAM has two key benefits for touch screen applications compared to biometrics (such as fingerprint, face, iris, hand, and ear) techniques regarding authentication. IBAM is safe against smudge attacks, although other biometrics are subject to attacks because duplication for them may occ- . such as fingerprints. For touch screen devices, IBAM does not need extra hardware, whereas biometrics-based authentication systems specific hardware is essential, like a fingerprint reader. Therefore, we assume that IBAM is a fair choice in real-world applications for touch-based devices and could be provided as an alternative for entering the PIN in certain cases.

When the user chooses 0 as his first PIN code digit, then the hacker has the option to choose 0-9 as the second digit of the user's PIN code. Suppose that the first digit is x, where $x \in S = \{0, 1....9\}$. For every $x \in S$, let us define S_x as the set of all possible choices for the digit x, then $|S_x| = 10$,

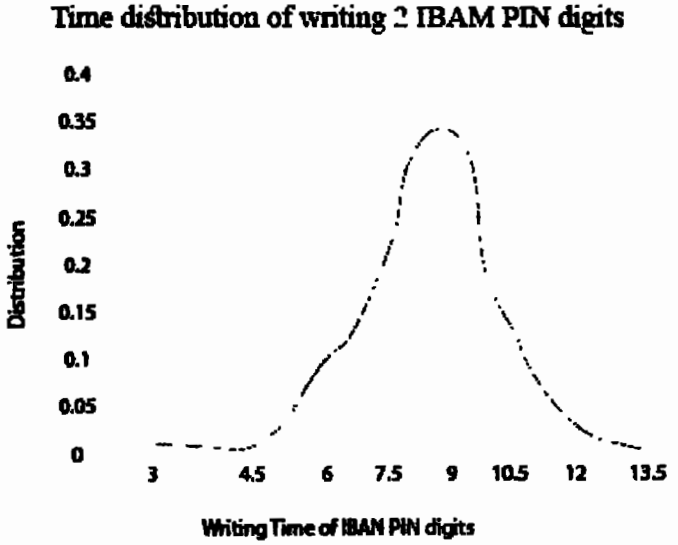

Figure 7.11: The time distribution of writing 2 IBAM PIN.

the following equation is obtain

$$\text{Total choices} = \sum_{x \in S} |S_x| = 100 \tag{7.1}$$

7.4 Comparison of IBAM

For mobile scenarios, IBAM in comparison with other emerging state-of-the-art biometric techniques regarding authentication. For each sample, Table 7.6 contains details related to the verification process and verification output in terms of EER. For the case of handwritten signatures [186] the EER performance was 5.04%. The limitation of this approach is that EER was not calculated - - the trained attackers. Handwritten digits recognition system was developed by [187, 188] in both of these approaches the EER for the random attack was not calculated. IBAM was tested on random and skilled. A skilled attack means that the attacker knows the PIN code generation technique, but IBAM confirms the biometric features of the user while writing the correct code digit.

Table 7.7 presents the comparison of IBAM technique with different authentication systems regarding security analysis. The comparison is based on Shoulder surfing, smudge attack, Random password, and biometrics. Shoulder surfing and smudge attacks are very common and easy for

Table 7.6: Comparison of related work of IBAM

Study	Method	Classifier	Random Attack	Skilled Attack	Participants
Sae-Bae et al. [186]	Handwritten Signatures	Manhattan Distance	-	EER = 4.84%	20
Nguyen et al.[81]	Handwritten Digits	Dynamic Time Wraping	-	EER = 4.84%	20
Tolosana et al. [187]	Handwritten Digits	Dynamic Time Wraping	-	EER = 5.5%	93
Kutzner et al. [188]	Handwritten Characters	K-Nearest Neighbor	-	FAR = 10.42% FRR = unknown	32
IBAM	Handwritten Digits	CNN	EER=2.6%	EER=4.6%	30

the attacker as they don't require any extra software or any knowledge about the authentication system. [189] and [181] uses multi-factor technique to secure authentication mechanism. With the use of a multi-factor system, the attacker has to break more than one line of defense to get to the original pattern or code to unlock the mobile device.

Table 7.7: Comparison of related work w.r.t. attacks

Ref.	Shoulder Attack	Biometric	Random Password	Smudge Attack	Accuracy	Multi-Factor	Classifier
[190]	✓	✓	✗	✓	91.0%	✗	CNN
[189]	✓	✓	✗	✗	99.06%	✓	CCV feature
[181]	✓	✓	✗	✓	98.58%	✓	CNN
[191]	✓	✓	✗	✓	91.0%	✗	LSTM
IBAM	✓	✓	✓	✓	98.32%	✓	CNN

7.5 Summary

In this chapter, as a major contribution a machine learning instruction basis authentication (IBAM) system is proposed, which enables the user to input a different PIN each time they log in. A collection of effective features that effectively record behavioral data are used while entering PIN codes on touch displays. This technique regarding the authentication of touchscreen appliances

presents IBAM(two-factor authentication technique) and illustrates the capability regarding the utilization of special attributes in drawing digits for the authentication of the user. With something you process authentication factor, the PIN codes digits should be processed by the user, and then he has to draw it on the screen instead of typing it. The chance of a smudge attack is neglected in the IBAM case as the user has to enter a new PIN codes digit every time he logins. Even if the PIN codes are shoulder surfed by an attacker, he has to draw the PIN codes according to the user's touch behaviors. IBAM increases the protection and usability of such devices compared to current passwords/PINs/pattern-based systems as it is non-vulnerable to attacks(shoulder surfing and smudge). The results show that IBAM attained an EER of 4.6% if the attacker recognized the user's PIN earlier. For the recognition of handwriting and verification of the writer, we expect to implement evolving deep learning architectures in the future. The extension of our scheme to validate both digits and letters would be another worthwhile endeavor.

Chapter 8

Conclusion and Future Work

We addressed the issues of user authentication on smartphones in this dissertation by presenting behavioral biometric-based methods that are efficient, resilient, user-friendly, and hardware-friendly as a replacement for existing authentication processes. This study examined the usefulness of using a dynamic behavioral user authentication strategy to recognize individuals as well as participant approval, which may have an impact on adoption in the future. The design was built around how users interact with touchscreen devices using their fingers. It also made use of the idea that various characteristics are produced when users move their fingers over touchscreen mobile devices while performing the authentication.

8.1 Summary

For smartphone user authentication, we have proposed multiple schemes. We evaluated the security, robustness, and usability of our suggested techniques and documented the results in this thesis. Results attained show a favorable indication of user approval. Our solutions authenticate users with little or no explicit user cooperation, which is what distinguishes them as being better and more distinctive. Additionally, all of our solutions make use of already-existing hardware, so they can all be used with the majority of smartphones on the market right now.

Pattern lock is mostly used by mobile users to unlock the device. The main drawback of this authentication scheme is the less password space, as the user has to redraw the same pattern on every authentication attempt. To overcome the pattern lock system's flaws, this thesis introduces a graphical authentication system called Operational Grid in chapter 5, which uses the fifth level of

authentication factor (Op-Grid). It's an effective and secure authentication solution for consumer devices that can protect user credentials even in the presence of recording cameras in public locations. OP-Grid is a graphical pad surrounded by a 7-11 grid matrix with a background image that varies each time the module is used. The resultant pattern is created by performing mathematical operations i.e. addition and subtraction on the numbers entered by the user during registration and the numbers provided by the server. Behavioral traits that distinguish each sequence input as authentic or imposter user were collected from these data using an SVM learning classifier. The obtained results show the value of FAR 4.36 and FRR 5.03.

An authentication scheme i.e. Processed Pattern Authentication(PPA) proposed in chapter 6 combines the behavior authentication and "something you process" authentication factor in a graphical box. It has two lines of defense, firstly the unique pattern indicator that shows a different value to the user at every login attempt, and secondly, if the pattern checker verifies the pattern correctly then, it authenticates the user based on touch behavior features. The proposed scheme for two-class classification chose to consider Artificial Neural Networks. The accuracy in our example is 0.75% and the error rate is 0.25%, so a high percentage of instances can be correctly labeled by the model.

Mobile users also authenticate in public places by drawing the PIN numbers on the lock screen, chapter 7 proposed a multi-dimensional behavior handwritten lock system i.e. Instructional handwritten authentication based on machine learning(IBAM). First, the user must compute the PIN code values, utilizing the "something you process" feature for authentication. Something you process factor also known as formula base authentication technique provides secure authentication against shoulder surfing attack, as a user on every login, enters a different password. For writer verification, the CNN classifier was trained. EER is 13.6% under shoulder surfing attack. The increased success rate is unsurprising given the attackers' extensive awareness of the user's drawing actions along with the PIN. Despite this, the framework refused attackers 86.4% of the time. These findings suggest that IBAM can help to reduce the risk of shoulder surfing.

The following is a list of the current dissertation conclusion.

8.1.1 Improving Authenticity Accuracy

One of the most crucial components of the authentication process that has been extensively researched is the very accurate identification of legitimate personnel. More particular, one of the common problems with the existing authentication mechanism is a stolen password attack. The

proposed techniques, Op-Grid (chapter 5) and PPA (chapter 6) are shown to significantly improve the accuracy rate in the authentication process.

8.1.2 Stop Password Changes by Malicious Users

Unauthorized users frequently alter the existing password in stolen password attacks in an effort to dominate and manage authentication procedures. The authentication accuracy was harmed by this gap. The proposed techniques fill in this gap, which forbids any unwanted password changes.

8.1.3 Behavioral features of the users during authentication

The behavioral features of the users while typing the pattern lock (IBAM Chapter 7) and drawing the pattern (Op-Grid chapter5, PPA chapter6), give extra security to the authentication process.

8.2 Future work

Based on the findings acquired through this thesis we have highlighted several potential research directions to increase the security of authentication systems based on behavioral biometrics. Despite significant advances in mobile biometrics, including the work reported in this thesis, there are still several difficulties that need to be addressed.

8.2.1 Performance Analysis

We'll assess our final proof-of-concept applications using a variety of performance metrics i.e, implementation issues on smartphones, accuracy, memory, and CPU overhead. We'll also aim to resolve the accessibility vs. performance trade, i.e., how many patterns the user needs to register for training and which classifier performs best depending on that number. Mobile devices must with the issue of performance in the authentication process due to hardware and memory constraints. In comparison to desktops, mobile devices can take longer to authenticate users.

8.2.2 Usability Analysis

To further evaluate the usability of our methods, we will conduct additional structured/semi-structured interviews as part of our usability analysis. We can suggest the following basic process

for creating a flexible authentication solution to a particular case once our research goals have been met:

- Characterizing the context-based risk of the target scenario and developing context-sensing algorithms to capture these aspects
- Evaluating the target scenario's security and usability needs and determining how to modify the authentication system accordingly
- Resolving exceptions of potential false detection of context sensing techniques or implicit authentication. The design of the user interface (UI), the user-device interaction design, the way data is collected, the design of the authentication protocol and other elements may all have an impact on how usable a biometric authentication system is.

8.2.3 Consistency Analysis

Any biometric-based authentication method's performance fluctuates over time due to noted within-person differences caused by a variety of factors such as context and environment. Consider the effect of being inebriated on the system's accuracy. Furthermore, aging and mental and/or physical health have an impact on accuracy. To assess the impact of aging and the user's mental and/or physical health conditions on our proposed methods, more research is required. To avoid the continual deterioration in the performance of the authentication solutions, research on possible approach(es) to eliminate the impacts of variations in health and age is also required.

8.2.4 Adversarial and Security Analysis

In general, research papers on mobile biometrics focus solely on the proposed authentication system's performance accuracy, ignoring the security analysis. As a result, no research into their resistance to various threats has been done. We have tested the security of our proposed methods with two of the attacks, i.e. shoulder surfing and smudge attack. We'll test the robustness of all of our prototypes against a variety of attacks in a variety of adversarial settings, and report on their accuracy in the light of random, targeted, and controlled attacks. The creation of an appropriate biometric data processing algorithm is also essential for the system to function accurately and efficiently to gain widespread user approval. Research on advanced algorithms should continue to enhance efficiency, accuracy in usability, security, and privacy all at once. Many banking mobile applications installed on users' mobile devices use two-factor authentication, but in 2016 [192] [193]an Android malware was able to circumvent this security measure. Two-factor authentication

codes, or SMS-based verification codes, can be intercepted by malware and forwarded to the attacker. This threat can evolve to access the biometric reference template that is kept on the mobile device in the case of biometric-based authentication and communicate it to the attacker. Employing policy-enforcement access control techniques suitable for resource-constrained mobile devices is one research direction to stop this kind of attack.

8.3 Final Thoughts

Due to the difficulty of an attacker replicating biometric features, the use of biometric authentication has proven to be a successful method of protecting user information. Because physiological biometrics are so sensitive, users of these devices have begun to express increasing worries about the privacy of the information collected. The majority of users have decided to forego using physiological biometric authentication as a result. Instead, behavioral biometrics are used to identify and authenticate individuals on smart devices. We have presented strategies for simple and silent smartphone user identification using behavioral biometrics in this research. We studied and integrated innovative behaviors (requiring fresh data) for the evaluation rather than tackling the problem with existing methodologies (old datasets). The individual being authenticated must be present at the time and location of authentication when using behavior biometrics. Universality, uniqueness, permanence measurability (collectability), performance, and acceptance are some of the unique functionalities of biometrics. The majority of people believe that biometrics are largely beneficial. Security is one of the key benefits of biometrics since it demonstrates how accurately and carefully people handle their data. This thesis contributes to the emerging trend of investigating mobile authentication as biometric identification. Furthermore, all of our proposed solutions make use of built-in smartphone sensors, obviating the need for any additional specialized hardware.

Bibliography

[1] D. West, "Invention and the mobile economy," *Brookings Institution Policy Report, Issues in Technology Innovation*, 2013.

[2] A. Rodríguez, R. Sañudo, M. Miranda, A. Gómez, and J. Benavente, "Smartphones and tablets applications in railways, ride comfort and track quality. transition zones analysis," *Measurement*, vol. 182, p. 109644, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S026322412100614X

[3] Z. Hu and Y. Xiang, "Who is the chief culprit, loneliness, or smartphone addiction? evidence from longitudinal study and weekly diary method," *International Journal of Mental Health and Addiction*, pp. 1–16, 2022.

[4] D. Agarwal and A. Bansal, "An alignment-free non-invertible transformation-based method for generating the cancellable fingerprint template," *Pattern Analysis and Applications*, pp. 1–16, 2022.

[5] C. Pope, "Biometric data collection in an unprotected world: Exploring the need for federal legislation protecting biometric data," *JL & Pol'y*, vol. 26, p. 769, 2018.

[6] A. B. Pandey, A. Tripathi, and P. C. Vashist, "A survey of cyber security trends, emerging technologies and threats," *Cyber Security in Intelligent Computing and Communications*, pp. 19–33, 2022.

[7] E. Kim, J.-S. Lin, and Y. Sung, "To app or not to app: Engaging consumers via branded mobile apps," *Journal of Interactive Advertising*, vol. 13, no. 1, pp. 53–65, 2013.

[8] D. Chaffey, "Mobile marketing statistics compilation," https://www.smartinsights.com/mobile-marketing/mobile-marketing-analytics/mobile-marketing-statistics/, accessed March 1, 2019.

[9] S. Arun Kumar, R. Ramya, R. Rashika, and R. Renu, "A survey on graphical authentication system resisting shoulder surfing attack," in *Advances in Artificial Intelligence and Data Engineering*. Springer, 2021, pp. 761–770.

[10] X. Bultel, J. Dreier, M. Giraud, M. Izaute, T. Kheyrkhah, P. Lafourcade, D. Lakhzoum, V. Marlin, and L. Motá, "Security analysis and psychological study of authentication methods with pin codes," in *2018 12th International Conference on Research Challenges in Information Science (RCIS)*. IEEE, 2018, pp. 1–11.

[11] R. Cappelli, D. Maio, A. Lumini, and D. Maltoni, "Fingerprint image reconstruction from standard templates," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 29, no. 9, pp. 1489–1503, 2007.

[12] A. Hern, "Hacker fakes german minister's fingerprints using photos of her hands," *The Guardian*, vol. 30, 2014.

[13] L. Bošnjak and B. Brumen, "Shoulder surfing experiments: A systematic literature review," *Computers & Security*, p. 102023, 2020.

[14] R. Duezguen, P. Mayer, S. Das, and M. Volkamer, "Towards secure and usable authentication for augmented and virtual reality head-mounted displays," *arXiv preprint arXiv:2007.11663*, 2020.

[15] M. Conti, P. P. Tricomi, and G. Tsudik, "De-auth of the blue! transparent de-authentication using bluetooth low energy beacon," in *European Symposium on Research in Computer Security*. Springer, 2020, pp. 277–294.

[16] A. Ometov, V. Petrov, S. Bezzateev, S. Andreev, Y. Koucheryavy, and M. Gerla, "Challenges of multi-factor authentication for securing advanced iot applications," *IEEE Network*, vol. 33, no. 2, pp. 82–88, March 2019.

[17] S. Shen, T. Kang, S. Lin, and W. Chien, "Random graphic user password authentication scheme in mobile devices," in *2017 International Conference on Applied System Innovation (ICASI)*, May 2017, pp. 1251–1254.

[18] T. Chen, M. Farcasin, and E. Chan-Tin, "Smartphone passcode prediction," *IET Information Security*, vol. 12, no. 5, pp. 431–437, 2018.

[19] A. Buriro, "Behavioral biometrics for smartphone user authentication," Ph.D. dissertation, University of Trento,Italy, 2017.

[20] S. A. Alsuhibany, "A camouflage text-based password approach for mobile devices against shoulder-surfing attack," *Security and Communication Networks*, vol. 2021, 2021.

[21] B. L. Muhammad-Bello, O. P. Lewu, S. Misra, A. K. Garg, J. Oluranti, and R. Maskeliunas, "ireportnow: A mobile-based lost and stolen reporting system," in *Recent Innovations in Computing*. Springer, 2022, pp. 753–766.

[22] A. Annavarapu, S. Borra, and R. Thanki, "Progression in biometric recognition systems and its security," *Recent Patents on Engineering*, vol. 16, no. 1, pp. 31–46, 2022.

[23] S. Pahuja and N. Goel, "State-of-the-art multi-trait based biometric systems: Advantages and drawbacks," in *International Conference on Emerging Technologies in Computer Engineering*. Springer, 2022, pp. 704–714.

[24] A. De Luca, A. Hang, E. Von Zezschwitz, and H. Hussmann, "I feel like i'm taking selfies all day! towards understanding biometric authentication on smartphones," in *Proceedings of the 33rd annual ACM conference on human factors in computing systems*, 2015, pp. 1411–1414.

[25] Z. Wang, F. Chen, N. Zhou, M. Ma, X. Li, Y. Guo, and D. Chen, "Identity authentication based on dynamic touch behavior on smartphone," in *2021 6th International Conference on Image, Vision and Computing (ICIVC)*. IEEE, 2021, pp. 469–474.

[26] R. V. Yampolskiy and V. Govindaraju, "Behavioural biometrics: a survey and classification," *International Journal of Biometrics*, vol. 1, no. 1, pp. 81–113, 2008.

[27] K. Ilgun, R. A. Kemmerer, and P. A. Porras, "State transition analysis: A rule-based intrusion detection approach," *IEEE transactions on software engineering*, vol. 21, no. 3, pp. 181–199, 1995.

[28] F. Apap, A. Honig, S. Hershkop, E. Eskin, and S. Stolfo, "Detecting malicious software by monitoring anomalous windows registry accesses," in *International Workshop on Recent Advances in Intrusion Detection*. Springer, 2002, pp. 36–53.

[29] A. K. Jain, A. A. Ross, and K. Nandakumar, *Introduction to biometrics*. Springer Science & Business Media, 2011.

[30] Sensors, "*https : //developer.android.com/guide/topics/sensors/sensors*$_o$*verview.html*."

[31] A. Buriro, B. Crispo, F. Delfrari, and K. Wrona, "Hold and sign: A novel behavioral bio-

metrics for smartphone user authentication," in *2016 IEEE security and privacy workshops (SPW)*. IEEE, 2016, pp. 276–285.

[32] M. Conti, I. Zachia-Zlatea, and B. Crispo, "Mind how you answer me! transparently authenticating the user of a smartphone when answering or placing a call," in *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*, 2011, pp. 249–259.

[33] A. Pramod, H. S. Naicker, and A. K. Tyagi, "Machine learning and deep learning: Open issues and future research directions for the next 10 years," *Computational Analysis and Deep Learning for Medical Care: Principles, Methods, and Applications*, pp. 463–490, 2021.

[34] W. Z. Khan, Y. Xiang, M. Y. Aalsalem, and Q. Arshad, "Mobile phone sensing systems: A survey," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 1, pp. 402–427, 2012.

[35] A. S. Patrick, A. C. Long, and S. Flinn, "HCI and security systems," in *CHI '03 extended abstracts on Human factors in computing systems - CHI '03*. ACM Press, 2003.

[36] Z. Zhang, H. Ning, F. Shi, F. Farha, Y. Xu, J. Xu, F. Zhang, and K.-K. R. Choo, "Artificial intelligence in cyber security: research advances, challenges, and opportunities," *Artificial Intelligence Review*, pp. 1–25, 2021.

[37] C. Wang, Y. Wang, Y. Chen, H. Liu, and J. Liu, "User authentication on mobile devices: Approaches, threats and trends," *Computer Networks*, vol. 170, p. 107118, 2020.

[38] D. Dasgupta, A. K. Nag, and A. Roy, "Adaptive multi-factor authentication system," Mar. 6 2018, uS Patent 9,912,657.

[39] https://www.smartinsights.com/mobile-marketing/mobile-marketing-analytics/mobile-marketing statistics/, "Mobile marketing statistics compilation," *Date of access:*, 15,Jan, 2020.

[40] V. Tsoukas, A. Gkogkidis, and A. Kakarountas, "A survey on mobile user perceptions of sensitive data and authentication methods," in *24th Pan-Hellenic Conference on Informatics*, ser. PCI 2020. New York, NY, USA: Association for Computing Machinery, 2020, p. 346–349. [Online]. Available: https://doi.org/10.1145/3437120.3437337

[41] S. A. Kumar, R. Ramya, R. Rashika, and R. Renu, "A survey on graphical authentication

system resisting shoulder surfing attack," in *Advances in Artificial Intelligence and Data Engineering*. Springer, 2021, pp. 761–770.

[42] K. Gilhooly, "Biometrics: Getting back to business," *Computerworld, May*, vol. 9, p. 2005, 2005.

[43] Y. Li, X. Yun, L. Fang, and C. Ge, "An efficient login authentication system against multiple attacks in mobile devices," *Symmetry*, vol. 13, no. 1, p. 125, 2021.

[44] S. S. ul Hasan Naqvi and S. Afzal, "Operation code authentication preventing shoulder surfing attacks," in *2010 3rd International Conference on Computer Science and Information Technology*. IEEE, jul 2010.

[45] H. Bhanbhro, S. Z. Nizamani, S. R. Hassan, S. T. Bakhsh, and M. O. Alassafi, "Enhanced textual password scheme for better security and memorability," *INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS*, vol. 9, no. 7, pp. 209–215, 2018.

[46] T. G. Tan, P. Szalachowski, and J. Zhou, "Securing password authentication for web-based applications," *arXiv preprint arXiv:2011.06257*, 2020.

[47] A. Amiri Sani, "Schrodintext: Strong protection of sensitive textual content of mobile applications," in *Proceedings of the 15th Annual International Conference on Mobile Systems, Applications, and Services*. ACM, 2017, pp. 197–210.

[48] R. Fatima, N. Siddiqui, M. S. Umar, and M. H. Khan, "A novel text-based user authentication scheme using pseudo-dynamic password," in *Information and Communication Technology for Competitive Strategies*. Springer, 2019, pp. 177–186.

[49] H.-S. Choi, B. Lee, and S. Yoon, "Biometric authentication using noisy electrocardiograms acquired by mobile sensors," *IEEE Access*, vol. 4, pp. 1266–1273, 2016.

[50] I. Traoré, Y. Nakkabi, S. Saad, B. Sayed, J. D. Ardigo, and P. M. de Faria Quinan, "Ensuring online exam integrity through continuous biometric authentication," in *Information Security Practices*. Springer, 2017, pp. 73–81.

[51] S. Thavalengal, T. Nedelcu, P. Bigioi, and P. Corcoran, "Iris liveness detection for next generation smartphones," *IEEE Transactions on Consumer Electronics*, vol. 62, no. 2, pp. 95–102, 2016.

[52] S. Thavalengal and P. Corcoran, "User authentication on smartphones: Focusing on iris biometrics," *IEEE Consumer Electronics Magazine*, vol. 5, no. 2, pp. 87–93, 2016.

[53] K. Sharmila, V. Janaki, and A. Nagaraju, "A novel approach for emergency backup authentication using fourth factor," in *Innovations in Computer Science and Engineering*. Springer, 2017, pp. 313–323.

[54] W. Zhou, X. Yuan, W. Chai, and H. Ma, "Deep learning based attack on social authentication system," in *2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*. IEEE, 2019, pp. 982–986.

[55] M. R. Rizqi, A. Waluyo, G. M. Edgy, and S. U. Sunaringtyas, "Enhanced authentication mechanism for automated teller machine (atm) through implementation of soft two-factor authentication," in *Proceedings of the 3rd International Conference on Electronics, Communications and Control Engineering*, 2020, pp. 3–7.

[56] B. Saranraj, N. S. P. Dharshini, R. Suvetha, and K. U. Bharathi, "Atm security system using arduino," in *2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS)*. IEEE, 2020, pp. 940–944.

[57] L. Ginzberg, "User authentication system and method," Nov. 28 2006, uS Patent 7,143,440.

[58] R. V. Yampolskiy, "User authentication via behavior based passwords," in *2007 IEEE Long Island Systems, Applications and Technology Conference*. IEEE, may 2007.

[59] M. Eiband, M. Khamis, E. von Zezschwitz, H. Hussmann, and F. Alt, "Understanding shoulder surfing in the wild," in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems - CHI '17*. ACM Press, 2017.

[60] A. Alhothaily, C. Hu, A. Alrawais, T. Song, X. Cheng, and D. Chen, "A secure and practical authentication scheme using personal devices," *IEEE Access*, vol. 5, pp. 11 677–11 687, 2017.

[61] I. Muslukhov, Y. Boshmaf, C. Kuo, J. Lester, and K. Beznosov, "Know your enemy," in *Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services - MobileHCI '13*. ACM Press, 2013.

[62] K. Fujita and Y. Hirakawa, "A study of password authentication method against observing attacks," in *2008 6th International Symposium on Intelligent Systems and Informatics*, Sept 2008, pp. 1–6.

[63] A. Narayanan and V. Shmatikov, "Fast dictionary attacks on passwords using time-space tradeoff," in *Proceedings of the 12th ACM conference on Computer and communications security - CCS '05*. ACM Press, 2005.

[64] L. Bosnjak, J. Sres, and B. Brumen, "Brute-force and dictionary attack on hashed real-world passwords," in *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*. IEEE, may 2018.

[65] P. Syverson, "A taxonomy of replay attacks [cryptographic protocols]," in *Proceedings The Computer Security Foundations Workshop VII*. IEEE Comput. Soc. Press, 1994.

[66] J. Li, "Design of authentication protocols preventing replay attacks," in *2009 International Conference on Future BioMedical Information Engineering (FBIE)*. IEEE, dec 2009.

[67] I. Uusitalo, J. M. Catot, and R. Loureiro, "Phishing and countermeasures in spanish online banking," in *2009 Third International Conference on Emerging Security Information, Systems and Technologies*. IEEE, 2009.

[68] E. Kirda and C. Kruegel, "Protecting users against phishing attacks with AntiPhish," in *29th Annual International Computer Software and Applications Conference (COMPSAC'05)*. IEEE, 2005.

[69] M. M. Baig and W. Mahmood, "A robust technique of anti key-logging using key-logging mechanism," in *2007 Inaugural IEEE-IES Digital EcoSystems and Technologies Conference*. IEEE, feb 2007.

[70] M. Raza, M. Iqbal, M. Sharif, and W. Haider, "A survey of password attacks and comparative analysis on methods for secure authentication," *World Applied Sciences Journal*, vol. 19, no. 4, pp. 439–444, 2012.

[71] R. Biddle, S. Chiasson, and P. V. Oorschot, "Graphical passwords," *ACM Computing Surveys*, vol. 44, no. 4, pp. 1–41, aug 2012.

[72] B. Pinkas and T. Sander, "Securing passwords against dictionary attacks," in *Proceedings of the 9th ACM conference on Computer and communications security - CCS '02*. ACM Press, 2002.

[73] J. Patel and A. Patel, "A survey on different authentication schemes for session passwords," *International Journal of Scientific Research in Science, Engineering and Technology*, vol. 1, no. 6, 2015.

[74] T. Kwon and S. Na, "TinyLock: Affordable defense against smudge attacks on smartphone pattern lock systems," *Computers & Security*, vol. 42, pp. 137–150, may 2014.

[75] M. Hosseinzadeh, B. Vo, M. Y. Ghafour, and S. Naghipour, "Electrocardiogram signals-based user authentication systems using soft computing techniques," *Artificial Intelligence Review*, vol. 54, no. 1, pp. 667–709, 2021.

[76] P. Kumar, R. Saini, P. P. Roy, and D. P. Dogra, "A bio-signal based framework to secure mobile devices," *Journal of Network and Computer Applications*, vol. 89, pp. 62–71, 2017.

[77] A. Forget, "A world with many authentication schemes," Ph.D. dissertation, Carleton University, 2013.

[78] M. Harbach, A. De Luca, and S. Egelman, "The anatomy of smartphone unlocking: A field study of android lock screens," in *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, 2016, pp. 4806–4817.

[79] C. Jacomme and S. Kremer, "An extensive formal analysis of multi-factor authentication protocols," *ACM Trans. Priv. Secur.*, vol. 24, no. 2, Jan. 2021. [Online]. Available: https://doi.org/10.1145/3440712

[80] K. S. Walia, S. Shenoy, and Y. Cheng, "An empirical analysis on the usability and security of passwords," in *2020 IEEE 21st International Conference on Information Reuse and Integration for Data Science (IRI)*. IEEE, 2020, pp. 1–8.

[81] T. Nguyen, N. Sae-Bae, and N. Memon, "Draw-a-pin: Authentication using finger-drawn pin on touch devices," *Comput. Secur.*, vol. 66, pp. 115–128, 2017.

[82] Y. Ku, L. H. Park, S. Shin, and T. Kwon, "Draw it as shown: Behavioral pattern lock for mobile user authentication," *IEEE Access*, vol. 7, pp. 69 363–69 378, 2019.

[83] G. Ye, Z. Tang, D. Fang, X. Chen, W. Wolff, A. J. Aviv, and Z. Wang, "A video-based attack for android pattern lock," *ACM Trans. Priv. Secur.*, vol. 21, no. 4, Jul. 2018. [Online]. Available: https://doi.org/10.1145/3230740

[84] M. Alajmi, I. Elashry, H. S. El-Sayed, and O. S. Faragallah, "A password-based authentication system based on the captcha ai problem," *IEEE Access*, vol. 8, pp. 153 914–153 928, 2020.

[85] B. S. Saini, P. Singh, A. Nayyar, N. Kaur, K. S. Bhatia, S. El-Sappagh, and J. Hu, "A three-

step authentication model for mobile phone user using keystroke dynamics," *IEEE Access*, vol. 8, pp. 125 909–125 922, 2020.

[86] Y. Sun and S. Upadhyaya, "Synthetic forgery attack against continuous keystroke authentication systems," in *2018 27th International Conference on Computer Communication and Networks (ICCCN)*. IEEE, jul 2018.

[87] G. Kambourakis, D. Damopoulos, D. Papamartzivanos, and E. Pavlidakis, "Introducing touchstroke: keystroke-based authentication system for smartphones," *Security and Communication Networks*, vol. 9, no. 6, pp. 542–554, jul 2014.

[88] H. Khan, U. Hengartner, and D. Vogel, "Mimicry attacks on smartphone keystroke authentication," *ACM Transactions on Privacy and Security (TOPS)*, vol. 23, no. 1, pp. 1–34, 2020.

[89] D. Buschek, A. De Luca, and F. Alt, "Improving accuracy, applicability and usability of keystroke biometrics on mobile touchscreen devices," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, ser. CHI '15. New York, NY, USA: Association for Computing Machinery, 2015, p. 1393–1402. [Online]. Available: https://doi.org/10.1145/2702123.2702252

[90] A. Buchoux and N. Clarke, "Deployment of keystroke analysis on a smartphone," *ECU Publications*, 01 2008.

[91] H. Saevanee and P. Bhattarakosol, "Authenticating user using keystroke dynamics and finger pressure," in *2009 6th IEEE Consumer Communications and Networking Conference*. IEEE, jan 2009.

[92] S. Zahid, M. Shahzad, S. A. Khayam, and M. Farooq, "Keystroke-based user identification on smart phones," in *Lecture Notes in Computer Science*. Springer Berlin Heidelberg, 2009, pp. 224–243.

[93] S. seob Hwang, S. Cho, and S. Park, "Keystroke dynamics-based authentication for mobile devices," *Computers & Security*, vol. 28, no. 1-2, pp. 85–93, feb 2009.

[94] L. Li, X. Zhao, and G. Xue, "Unobservable re-authentication for smartphones," in *NDSS*, 2013.

[95] M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song, "Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 1, pp. 136–148, jan 2013.

[96] H. Xu, Y. Zhou, and M. R. Lyu, "Towards continuous and passive authentication via touch biometrics: An experimental study on smartphones," in *10th Symposium On Usable Privacy and Security (SOUPS 2014)*. Menlo Park, CA: USENIX Association, 2014, pp. 187–198.

[97] H. Wang, T. Chen, X. Liu, and J. Chen, "Exploring the hand and finger-issued behaviors toward natural authentication," *IEEE Access*, vol. 8, pp. 55 815–55 825, 2020.

[98] L. Fridman, S. Weber, R. Greenstadt, and M. Kam, "Active authentication on mobile devices via stylometry, application usage, web browsing, and GPS location," *IEEE Systems Journal*, vol. 11, no. 2, pp. 513–521, jun 2017.

[99] T. Sudhakar and M. Gavrilova, "Deep learning for multi-instance biometric privacy," *ACM Trans. Manage. Inf. Syst.*, vol. 12, no. 1, Dec. 2020. [Online]. Available: https://doi.org/10.1145/3389683

[100] S. Dargan and M. Kumar, "A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities," *Expert Systems with Applications*, vol. 143, p. 113114, 2020.

[101] A. Al Abdulwahid, N. Clarke, I. Stengel, S. Furnell, and C. Reich, "Continuous and transparent multimodal authentication: reviewing the state of the art," *Cluster Computing*, vol. 19, no. 1, pp. 455–474, 2016.

[102] R. Ryu, S. Yeom, S.-H. Kim, and D. Herbert, "Continuous multimodal biometric authentication schemes: A systematic review," *IEEE Access*, 2021.

[103] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A survey of machine and deep learning methods for internet of things (iot) security," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1646–1685, 2020.

[104] W. Meng, D. S. Wong, S. Furnell, and J. Zhou, "Surveying the development of biometric user authentication on mobile phones," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 3, pp. 1268–1293, 2014.

[105] C. Bo, L. Zhang, X.-Y. Li, Q. Huang, and Y. Wang, "Silentsense: silent user identification via touch and movement behavioral biometrics," in *Proceedings of the 19th annual international conference on Mobile computing & networking*, 2013, pp. 187–190.

[106] Y. Song, Z. Cai, and Z.-L. Zhang, "Multi-touch authentication using hand geometry and

behavioral information," in *2017 IEEE symposium on security and privacy (SP)*. IEEE, 2017, pp. 357–372.

[107] M. Ehatisham-ul Haq, M. A. Azam, U. Naeem, S. ur Rehman, and A. Khalid, "Identifying smartphone users based on their activity patterns via mobile sensing," *Procedia computer science*, vol. 113, pp. 202–209, 2017.

[108] Y. Liang, Z. Cai, J. Yu, Q. Han, and Y. Li, "Deep learning based inference of private information using embedded sensors in smart devices," *IEEE Network*, vol. 32, no. 4, pp. 8–14, 2018.

[109] M. Sajjad, S. Khan, T. Hussain, K. Muhammad, A. K. Sangaiah, A. Castiglione, C. Esposito, and S. W. Baik, "CNN-based anti-spoofing two-tier multi-factor authentication system," *Pattern Recognition Letters*, feb 2018.

[110] W. Li, Y. Wang, J. Li, and Y. Xiang, "Toward supervised shape-based behavioral authentication on smartphones," *Journal of Information Security and Applications*, vol. 55, p. 102591, 2020.

[111] G.-Y. Shin, D.-W. Kim, S.-S. Kim, and M.-M. Han, "Unknown attack detection: Combining relabeling and hybrid intrusion detection," *Comput. Mater. Continua*, 2021.

[112] M. Abuhamad, T. Abuhmed, D. Mohaisen, and D. Nyang, "Autosen: Deep-learning-based implicit continuous authentication using smartphone sensors," *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 5008–5020, 2020.

[113] M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song, "Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication," *IEEE transactions on information forensics and security*, vol. 8, no. 1, pp. 136–148, 2012.

[114] O. Alpar, "Intelligent biometric pattern password authentication systems for touchscreens," *Expert Systems with Applications*, vol. 42, no. 17-18, pp. 6286–6294, 2015.

[115] O. Alpar and O. Krejcar, "Pattern password authentication based on touching location," in *International conference on intelligent data engineering and automated learning*. Springer, 2015, pp. 395–403.

[116] L. Zhou, Y. Kang, D. Zhang, and J. Lai, "Harmonized authentication based on thumbstroke dynamics on touch screen mobile phones," *Decision Support Systems*, vol. 92, pp. 14–24, 2016.

[117] P. Samangouei, V. M. Patel, and R. Chellappa, "Facial attributes for active authentication on mobile devices," *Image and Vision Computing*, vol. 58, pp. 181–192, 2017.

[118] M. Ehatisham-ul Haq, M. A. Azam, U. Naeem, Y. Amin, and J. Loo, "Continuous authentication of smartphone users based on activity pattern recognition using passive mobile sensing," *Journal of Network and Computer Applications*, vol. 109, pp. 24–35, 2018.

[119] I. Olade, C. Fleming, and H.-N. Liang, "Biomove: Biometric user identification from human kinesiological movements for virtual reality systems," *Sensors*, vol. 20, no. 10, p. 2944, 2020.

[120] A. A. Bello, H. Chiroma, A. Y. Gital, L. A. Gabralla, S. M. Abdulhamid, and L. Shuib, "Machine learning algorithms for improving security on touch screen devices: a survey, challenges and new perspectives." *Neural Computing & Applications*, vol. 32, no. 17, 2020.

[121] J. Fierrez, A. Pozo, M. Martinez-Diaz, J. Galbally, and A. Morales, "Benchmarking touchscreen biometrics for mobile authentication," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 11, pp. 2720–2733, 2018.

[122] P. Lacharme and C. Rosenberger, "Synchronous one time biometrics with pattern based authentication," in *2016 11th International Conference on Availability, Reliability and Security (ARES)*. IEEE, 2016, pp. 260–265.

[123] L. G. Hafemann, R. Sabourin, and L. S. Oliveira, "Learning features for offline handwritten signature verification using deep convolutional neural networks," *Pattern Recognition*, vol. 70, pp. 163–176, 2017.

[124] Y. Li, J. Luo, S. Deng, and G. Zhou, "Cnn-based continuous authentication on smartphones with conditional wasserstein generative adversarial network," *IEEE Internet of Things Journal*, vol. 9, no. 7, pp. 5447–5460, 2021.

[125] L. G. Hafemann, R. Sabourin, and L. S. Oliveira, "Writer-independent feature learning for offline signature verification using deep convolutional neural networks," in *2016 international joint conference on neural networks (IJCNN)*. IEEE, 2016, pp. 2576–2583.

[126] S. M. Obaidullah, C. Halder, N. Das, and K. Roy, "A new dataset of word-level offline handwritten numeral images from four official indic scripts and its benchmarking using image transform fusion," *International Journal of Intelligent Engineering Informatics*, vol. 4, no. 1, pp. 1–20, 2016.

[127] V. Aubin, M. Mora, and M. Santos-Peñas, "Off-line writer verification based on simple graphemes," *Pattern Recognition*, vol. 79, pp. 414–426, 2018.

[128] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, and J. Ortega-Garcia, "Exploring recurrent neural networks for on-line handwritten signature biometrics," *Ieee Access*, vol. 6, pp. 5128–5138, 2018.

[129] X.-Y. Zhang, G.-S. Xie, C.-L. Liu, and Y. Bengio, "End-to-end online writer identification with recurrent neural network," *IEEE Transactions on Human-Machine Systems*, vol. 47, no. 2, pp. 285–292, 2016.

[130] S. Hochreiter and J. Schmidhuber, "Long short-term memory," *Neural computation*, vol. 9, no. 8, pp. 1735–1780, 1997.

[131] M. Taşkiran and Z. G. Çam, "Offline signature identification via hog features and artificial neural networks," in *2017 IEEE 15th International Symposium on Applied Machine Intelligence and Informatics (SAMI)*. IEEE, 2017, pp. 000 083–000 086.

[132] A. Vaddeti, D. Vidiyala, V. Puritipati, R. B. Ponnuru, J. S. Shin, and G. R. Alavalapati, "Graphical passwords: Behind the attainment of goals," *Security and Privacy*, vol. 3, no. 6, p. e125, 2020.

[133] A. V. Kayem, "Graphical passwords–a discussion," in *2016 30th International Conference on Advanced Information Networking and Applications Workshops (WAINA)*. IEEE, 2016, pp. 596–600.

[134] F. Tari, A. A. Ozok, and S. H. Holden, "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*, 2006, pp. 56–66.

[135] S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords: Effects of tolerance and image choice," in *Proceedings of the 2005 symposium on Usable privacy and security*, 2005, pp. 1–12.

[136] H. Sun, S. Chen, J. Yeh, and C. Cheng, "A shoulder surfing resistant graphical authentication system," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 2, pp. 180–193, March 2018.

[137] A. A. Cain and J. D. Still, "A rapid serial visual presentation method for graphical au-

thentication," in *Advances in Intelligent Systems and Computing*. Springer International Publishing, 2016, pp. 3–11.

[138] K. Irfan, A. Anas, S. Malik, and S. Amir, "Text based graphical password system to obscure shoulder surfing," in *2018 15th International Bhurban Conference on Applied Sciences and Technology (IBCAST)*. IEEE, 2018, pp. 422–426.

[139] Z. Yu, I. Olade, H.-N. Liang, and C. Fleming, "Usable authentication mechanisms for mobile devices: An exploration of 3d graphical passwords," in *2016 International Conference on Platform Technology and Service (PlatCon)*. IEEE, feb 2016.

[140] S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and longitudinal evaluation of a graphical password system," *International Journal of Human-Computer Studies*, vol. 63, no. 1-2, pp. 102–127, jul 2005.

[141] S. Wiedenbeck, J. Waters, L. Sobrado, and J.-C. Birget, "Design and evaluation of a shoulder-surfing resistant graphical password scheme," in *Proceedings of the working conference on Advanced visual interfaces - AVI '06*. ACM Press, 2006.

[142] R. Giot, M. El-Abed, and C. Rosenberger, "Keystroke dynamics authentication for collaborative systems," in *2009 International Symposium on Collaborative Technologies and Systems*. IEEE, 2009, pp. 172–179.

[143] A. M. Pietron and T. Han, "A case study of graphical passwords in a chinese university," in *Adjunct Publication of the 28th ACM Conference on User Modeling, Adaptation and Personalization*, 2020, pp. 175–180.

[144] A. Nayak and R. Bansode, "Analysis of knowledge based authentication system using persuasive cued click points," *Procedia Computer Science*, vol. 79, pp. 553–560, 2016.

[145] G. Y. Izadeen and S. Y. Ameen, "Smart android graphical password strategy: A review," *Asian Journal of Research in Computer Science*, pp. 59–69, 2021.

[146] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith, "Smudge attacks on smartphone touch screens," in *4th USENIX Workshop on Offensive Technologies (WOOT 10)*, 2010.

[147] C.-Y. Liu, S.-J. Ruan, Y.-R. Lai, and C.-Y. Yao, "Finger-vein as a biometric-based authentication," *IEEE Consumer Electronics Magazine*, vol. 8, no. 6, pp. 29–34, 2019.

[148] P. Sukumar and R. Gnanamurthy, "Computer aided detection of cervical cancer using pap

smear images based on adaptive neuro fuzzy inference system classifier," *Journal of Medical Imaging and Health Informatics*, vol. 6, no. 2, pp. 312–319, 2016.

[149] S. Krishnamoorthy, L. Rueda, S. Saad, and H. Elmiligi, "Identification of user behavioral biometrics for authentication using keystroke dynamics and machine learning," in *Proceedings of the 2018 2nd International Conference on Biometric Engineering and Applications*, 2018, pp. 50–57.

[150] K.-W. Tse and K. Hung, "Behavioral biometrics scheme with keystroke and swipe dynamics for user authentication on mobile platform," in *2019 IEEE 9th Symposium on Computer Applications & Industrial Electronics (ISCAIE)*. IEEE, 2019, pp. 125–130.

[151] D. J. Gunn, Z. Liu, R. Dave, X. Yuan, and K. Roy, "Touch-based active cloud authentication using traditional machine learning and lstm on a distributed tensorflow framework," *International Journal of Computational Intelligence and Applications*, vol. 18, no. 04, p. 1950022, 2019.

[152] Z. Sakhrawi, A. Sellami, and N. Bouassida, "Software enhancement effort estimation using correlation-based feature selection and stacking ensemble method," *Cluster Computing*, pp. 1–14, 2021.

[153] S. Gershon and H. Okonkwo, "Evaluating the sensitivity, specificity and clinical utility of algorithms of spatial variation in sub-epidermal moisture (sem) for the diagnosis of deep and early-stage pressure-induced tissue damage," *Journal of Wound Care*, vol. 30, no. 1, pp. 41–53, 2021.

[154] S. Boonkrong, "Internet banking login with multi-factor authentication," *KSII Transactions on Internet and Information Systems (TIIS)*, vol. 11, no. 1, pp. 511–535, 2017.

[155] D. Izumoto and Y. Yamazaki, "Security enhancement for touch panel based user authentication on smartphones," in *2019 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC)*. IEEE, 2019, pp. 218–223.

[156] T. Zhu, Z. Weng, G. Chen, and L. Fu, "A hybrid deep learning system for real-world mobile user authentication using motion sensors," *Sensors*, vol. 20, no. 14, p. 3876, 2020.

[157] S. Keykhaie and S. Pierre, "Mobile match on card active authentication using touchscreen biometric," *IEEE Transactions on Consumer Electronics*, vol. 66, no. 4, pp. 376–385, 2020.

[158] L. Janik, D. Chuda, and K. Burda, "Sgfa: A two-factor smartphone authentication mecha-

nism using touch behavioral biometrics," in *Proceedings of the 21st International Conference on Computer Systems and Technologies' 20*, 2020, pp. 35–42.

[159] F. Masood, A. Almogren, A. Abbas, H. A. Khattak, I. U. Din, M. Guizani, and M. Zuair, "Spammer detection and fake user identification on social networks," *IEEE Access*, vol. 7, pp. 68 140–68 152, 2019.

[160] S. Azad, M. Rahman, M. N. Ranak, B. K. Ruhee, N. N. Nisa, N. Kabir, A. Rahman, and J. M. Zain, "Vap code: A secure graphical password for smart devices," *Computers & Electrical Engineering*, vol. 59, pp. 99–109, 2017.

[161] A. Ghani, M. Bilal, A. Jolfaei *et al.*, "Multi-factor pattern implicit authentication," *IEEE Consumer Electronics Magazine*, 2021.

[162] J. K. Han, X. Bi, H. Kim, and S. S. Woo, "Passtag: a graphical-textual hybrid fallback authentication system," in *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security*, 2020, pp. 60–72.

[163] G.-C. Yang, "Passpositions: A secure and user-friendly graphical password scheme," in *2017 4th International Conference on Computer Applications and Information Processing Technology (CAIPT)*. IEEE, 2017, pp. 1–5.

[164] S. S. Hassan, S. Ullah, S. Afzal, M. A. Khan, M. A. Khan, and H. Akbar, "Servers voice graphical authentication," in *2015 12th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD)*. IEEE, 2015, pp. 2582–2586.

[165] C. Baadte and B. Meinhardt-Injac, "The picture superiority effect in associative memory: A developmental study," *British Journal of Developmental Psychology*, vol. 37, no. 3, pp. 382–395, 2019.

[166] J. Zheng and S. K. Chigurupati, "M-pattern: A novel scheme for improving the security of android pattern unlock against smudge attacks," *ICT Express*, vol. 5, no. 3, pp. 192–195, 2019.

[167] M. Wazid, S. Zeadally, and A. K. Das, "Mobile banking: evolution and threats: malware threats and security solutions," *IEEE Consumer Electronics Magazine*, vol. 8, no. 2, pp. 56–60, 2019.

[168] Y. Sun, Q. Gao, X. Du, and Z. Gu, "Smartphone user authentication based on holding posi-

tion and touch-typing biometrics," *Comput. Mater. Continua*, vol. 3, no. 61, pp. 1365–1375, 2019.

[169] E. Mbunge and T. Rugube, "A robust and scalable four factor authentication architecture to enhance security for mobile online transaction," *International journal of scientific & technology research*, vol. 7, no. 3, pp. 139–143, 2018.

[170] E. A. Sağbaş, S. Korukoglu, and S. Balli, "Stress detection via keyboard typing behaviors by using smartphone sensors and machine learning techniques," *Journal of medical systems*, vol. 44, no. 4, pp. 1–12, 2020.

[171] S. H. Ebenuwa, M. S. Sharif, M. Alazab, and A. Al-Nemrat, "Variance ranking attributes selection techniques for binary classification problem in imbalance data," *IEEE Access*, vol. 7, pp. 24 649–24 666, 2019.

[172] J. Zhao, Q. Hu, G. Liu, X. Ma, F. Chen, and M. M. Hassan, "Afa: Adversarial fingerprinting authentication for deep neural networks," *Computer Communications*, vol. 150, pp. 488–497, 2020.

[173] T. Hachaj and P. Mazurek, "Comparative analysis of supervised and unsupervised approaches applied to large-scale "in the wild" face verification," *Symmetry*, vol. 12, no. 11, p. 1832, 2020.

[174] E. S. Alkronz, K. A. Moghayer, M. Meimeh, M. Gazzaz, B. S. Abu-Nasser, and S. S. Abu-Naser, "Prediction of whether mushroom is edible or poisonous using back-propagation neural network," *International Journal of Corpus Linguistics*, 2019.

[175] H. Gascon, S. Uellenbeck, C. Wolf, and K. Rieck, "Continuous authentication on mobile devices by analysis of typing motion behavior," *Sicherheit 2014–Sicherheit, Schutz und Zuverlässigkeit*, 2014.

[176] C.-C. Chang and C.-J. Lin, "Libsvm: A library for support vector machines," *ACM transactions on intelligent systems and technology (TIST)*, vol. 2, no. 3, pp. 1–27, 2011.

[177] Y. Liang, S. Samtani, B. Guo, and Z. Yu, "Behavioral biometrics for continuous authentication in the internet-of-things era: An artificial intelligence perspective," *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 9128–9143, 2020.

[178] R. Tolosana, R. Vera-Rodriguez, and J. Fierrez, "Biotouchpass: Handwritten passwords for touchscreen biometrics," *IEEE Transactions on Mobile Computing*, 2019.

[179] S.-Y. Shin, Y.-W. Kang, and Y.-G. Kim, "Android-gan: Defending against android pattern attacks using multi-modal generative network as anomaly detector," *Expert Systems with Applications*, vol. 141, p. 112964, 2020.

[180] Q. Yue, Z. Ling, X. Fu, B. Liu, W. Yu, and W. Zhao, "My google glass sees your passwords," *Proceedings of the Black Hat USA*, 2014.

[181] Z. Li, H. Lee, Y. Lee, S. Yoon, B. Bae, and H.-J. Choi, "Handwritten one-time password authentication system based on deep learning," *Journal of Internet Computing and Services*, vol. 20, no. 1, pp. 25–37, 2019.

[182] M. S. Rudolph, N. B. Toussaint, A. Katabarwa, S. Johri, B. Peropadre, and A. Perdomo-Ortiz, "Generation of high-resolution handwritten digits with an ion-trap quantum computer," *Physical Review X*, vol. 12, no. 3, p. 031010, 2022.

[183] M. Shahzad, A. X. Liu, and A. Samuel, "Secure unlocking of mobile touch screen devices by simple gestures: you can see it but you can not do it," in *Proceedings of the 19th annual international conference on Mobile computing & networking*, 2013, pp. 39–50.

[184] J. Sun, R. Zhang, J. Zhang, and Y. Zhang, "Touchin: Sightless two-factor authentication on multi-touch mobile devices," in *2014 IEEE conference on communications and network security*. IEEE, 2014, pp. 436–444.

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

[186] N. Sae-Bae and N. Memon, "Online signature verification on mobile devices," *IEEE transactions on information forensics and security*, vol. 9, no. 6, pp. 933–947, 2014.

[187] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, and J. Ortega-Garcia, "Incorporating touch biometrics to mobile one-time passwords: Exploration of digits," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops*, 2018, pp. 471–478.

[188] T. Kutzner, F. Ye, I. Bönninger, C. Travieso, M. K. Dutta, and A. Singh, "User verification using safe handwritten passwords on smartphones," in *2015 Eighth International Conference on Contemporary Computing (IC3)*. IEEE, 2015, pp. 48–53.

[189] P. Thoopsamut and B. Limthanmaphon, "Handwritten signature authentication using color

coherence vector and signing behavior," in *Proceedings of the 2019 2nd international conference on information science and systems*, 2019, pp. 38–42.

[190] J. Peiqing, "Pinwrite: A new smartphone authentication scheme using handwriting recognition," Ph.D. dissertation, Waseda University, 2018.

[191] L. Fang, H. Zhu, B. Lv, Z. Liu, W. Meng, Y. Yu, S. Ji, and Z. Cao, "Handitext: Handwriting recognition based on dynamic characteristics with incremental lstm," *ACM Transactions on Data Science*, vol. 1, no. 4, pp. 1–18, 2020.

[192] L. Stefanko, "Android banking trojan masquerades as flash player and bypasses 2fa," Online, Mar. 2016. [Online]. Available: https://www.welivesecurity.com/2016/03/09/android-trojan-targets-online-banking-users/

[193] D. Palmer, "This new android malware bypasses multi-factor authentication to steal your passwords," Online, Jun. 2016. [Online]. Available: https://www.zdnet.com/article/this-new-android-malware-bypasses-multi-factor-authentication-to-steal-your-passwords/