Impact of video surveillance system on ATM PIN security

Authors

Dilanka Perera : 15020509

Harinda Samarasekara : 15020657

Piyumi Seneviratne : 15020721

Supervisor : Dr. C.I.Keppetiyagama

Co-supervisor : Dr. Kasun de Zoysa

Advisor : Mr. Kenneth Thilakarathna

February 2020

This dissertation is submitted to the University of Colombo School of Computing in partial fulfillment of the requirements for the Degree of Bachelor of Science Honours in Information Systems.

Declaration

I, D.N. Perera (2015/IS/050) hereby certify that this dissertation entitled Impact of video surveillance system on ATM PIN security is entirely my own work and it has never been submitted nor is currently been submitted for any other degree.

.....
Signature of Candidate Date :

I, P.H.Samarasekara (2015/IS/065) hereby certify that this dissertation entitled Impact of video surveillance system on ATM PIN security is entirely my own work and it has never been submitted nor is currently been submitted for any other degree.

.....
Signature of Candidate Date :

I, T.P.W Seneviratne (2015/IS/072) hereby certify that this dissertation entitled Impact of video surveillance system on ATM PIN security is entirely my own work and it has never been submitted nor is currently been submitted for any other degree.

.....
Signature of Candidate Date :

I, Dr. C.I.Keppetiyagama, certify that I supervised this dissertation entitled Impact of video surveillance system on ATM PIN security conducted by D.N. Perera, P.H.Samarasekara, T.P.W Seneviratne in partial fulfillment of the requirements for the degree of Bachelor of Science Honours in Information Systems.

.....
Signature of Supervisor Date :

I, Dr. Kasun de Zoysa, certify that I supervised this dissertation entitled Impact of video surveillance system on ATM PIN security conducted by D.N. Perera, P.H.Samarasekara, T.P.W Seneviratne in partial fulfillment of the requirements for the degree of Bachelor of Science Honours in Information Systems.

.....

Signature of Co-Supervisor Date :

Abstract

In Sri Lanka, it is a common practice to install wall mounted surveillance cameras in ATM cubicles. Surveillance cameras are installed to detect and/or monitor the situation and people inside the ATM cubicle for safety reasons and as a precautionary measure against the disputes regarding the dispense of cash. However, the researcher show that ad-hoc implementation of surveillance cameras inside an ATM cubicle has a potential threat to ATM PIN security. In the course of the background study the researchers identified that, in some cases, the PIN entering process is clearly visible through the surveillance camera footage. Researchers also show that it is possible to infer the ATM PIN simply by observing the forearm movement pattern even when the PIN pad is not visible on the video footage. In most banks, the surveillance camera footage are available to the personnel who are not cleared to access the banking system. In addition, banks operate under the premise that the PIN number is known only to the customer. Elaborate systems, such as HSMs and PIN Mailers, are in place to ensure that even the banking staff is not privy to the PIN number of a customer. Therefore, the potential exposure of the PIN number of a customer to a third party through the CCTV camera footage can be considered as a severe security violation in the electronic banking system. For this PIN inference process researchers have developed a programme using OpenCV and Python. Furthermore researchers have have propose a novel method to identify the key press events using the gradient of forearm movements.

Acknowledgement

First and foremost, we would like to express our sincere gratitude to our research supervisor Dr. C.I. Keppitiyagama, senior lecturer, University of Colombo School of Computing, research co-supervisor Dr. Kasun de Zoysa , senior lecturer, University of Colombo School of Computing.

We would like to extend my deepest gratitude to our advisers Mr. Kenneth Thilakarathna, lecturer, University of Colombo School of Computing for providing us with immense support, continuous guidance and supervision throughout the research and Dr. Primal Wijesekera, our co-supervisor for providing us with useful feedback, immense support and encouragement to carry out the research.

It is with much respect to further express our thanks to Dr. Chaminda Ranasinghe, CEO at IDEAHUB (pvt) LTD. for providing us with insightful information on the ATM system information technology and services industry.

Furthermore, we would also like to acknowledge Mr. Wasantha Jayasekara, Senior Manager IT (R&D), Bank of Ceylon Sri Lanka, Dr. Amal Illesinghe, Mr. Neelaka Aluthge of Commercial Bank of Sri Lanka and Mrs. P.D.T.L Pahalawatta, Senior Assistant Director, Central Bank of Sri Lanka for the support and cooperation rendered to us during the background study.

And also we would express our gratitude for all the student volunteers from University of Colombo School of Computing, who participated in our Manual Analysis survey and providing our research with valuable support.

Table of Contents

List of Figures

List of Tables

List of Acronyms

ATM Automated Teller Machine

CBSL Central Bank of Sri Lanka

HSM Hardware Security Modules

HSV Hue Saturation Value

LMK Local Master Key

OTI Optimal Transposition Index

PCI Payment Card Industry

PIN Personal Identification Number

RGB Red Green Blue

RTGS Real-Time Gross Settlement

UCSC University of Colombo School of Computing

Chapter 1

Introduction

At present with the advancement of technology, security has become a critical factor in the application of information systems. Among the different controlling methodologies of security, placing a surveillance camera is used as a physical control. Researchers have observed that the majority of the widespread network of ATM cubicles are equipped with a wall-mounted surveillance camera.

During the course of the research, local and international guidelines for the installation of surveillance cameras inside the ATM cubicles was reviewed. For a local guideline, CBSL only suggests banks to install surveillance cameras as a security measure. Payment Card Industry Security Standards Council(PCI) issues guidelines and best practices for ATM and PIN security. The PCI PTS POI ATM Security Guidelines [1] states, "the location for camera installation at ATMs should be carefully chosen to ensure that images of keypad entry are not captured and the camera should support the detection of the attachment of alien devices to the ATM front view and possess the ability to generate an alarm for remote monitoring if the camera is blocked or otherwise disabled".

However, there are many incidents where the keypad and the keypad entering process is visible through the surveillance camera footage due to ad hoc installation practice of surveillance cameras in ATM cubicles. This keypad entries might contain security-sensitive information such as PIN of an ATM customer. According to the Central Bank of Sri Lanka (CBSL) [2], the PIN is a piece of confidential customer information. Therefore, banks and other financial institutes use Hardware Security Modules (HSMs) for PIN generation, management and validation. PIN Mailers are used to securely print the PIN without revealing it even to the trusted employees in the bank. Hence, this system is mainly operating under the trust assumption that the PIN is secured and kept in private by both the system and the customer to ensure the security requirement of confidentiality. Even though banks heavily invest in employing HSMs for the PIN generation process to ensure the confidentiality of the PIN, ad hoc implementation of surveillance cameras might

contravene that objective. Consequently, the PIN is no longer confidential and it violates the principal assumption of the ATM system.

The existing literature does not specifically study the real-world scenario and address the potential threat to security-sensitive information resulting from the ad-hoc installation of surveillance cameras. However, previous studies show the possibility of inferring keyboard inputs using video footage. These videos are captured with a direct line of sight towards the keyboard and key press were identified by either analysing the fingertip movement [3] or the occluded area of the keyboard by hand [4] or using the identification of the key popup events [5]. In either situation, the keyboard or reflection of the keyboard is visible to the attackers. Shukla et al [6] shows that the potential of inferring keyboard inputs of a smartphone by tracking the point on the palm of the person who is using the smartphone in a situation where the keypad is not visible to the attacker. Yet in that study, it creates a favourable environment for the attacker to capture the palm. In this research, real-world ATM surveillance video footage and installation processes were examined comprehensively. Based on the real-world observations the PIN entering processes was captured under unfavourable situation for the attacker, where both PIN pad and fingertips are not visible to the attacker. Moreover, the attacker does not possess the ability to change the static position of the surveillance camera. This research was carried out to identify the potential threat and consequences of the ad-hoc installation of wall-mounted surveillance cameras inside ATM cubicles.

1.1 Problem Statement

It can be observed that surveillance cameras are widely used as a physical control for monitoring and inspecting any unusual activity or event happen indoors and outdoors. Most of the time these cameras are placed to capture or monitor peoples' movement. However, the exposure of information and data through these surveillance systems did not get sufficient attention. One such situation is the installation of surveillance cameras inside ATM cubicles.

This ATM scenario is a prime example for the application of technical security controls alongside the physical security controls in the real-world. According to PCI PTS POI ATM Security Guidelines[1], the location for camera installation at ATMs should be carefully chosen to ensure that images of keypad entry are not captured. However, it was identified that there are many incidents where the PIN entering process is visible through the camera footage due to ad-hoc installation practice of surveillance cameras in ATM cubicles. This research is carried out to explore the impact of surveillance cameras on information security of an ATM

system.

1.2 Research Questions

In this research, it is ordered on determining the capability of inferring the ATM PIN through the visual analysis of CCTV video footage. That is, in concerning the situation where the camera is placed in a static position. However, the degree to which the PIN can be inferred varies depending on different conditions. Accordingly, this aspect is addressed by the question, **"What is the potential to discover the ATM PIN through visual analysis of surveillance camera footage?"**.

Due to the exposure of the ATM PIN as an implication of ad hoc installation of CCTV cameras, it may result in negative consequences to the banking system. Hence, it is important to precisely identify the impact of these negative consequences to ensure the ATM PIN security in the banking information system. Thus, this aspect is addressed by the question, **"What are the threats of revealing the ATM PIN and what is the impact on the banking system?"**.

1.3 Goals and Objectives

1.3.1 Goals

- Investigate whether the ad-hoc installation of surveillance cameras cause any threat to ATM PIN security.

1.3.2 Objectives

- Analyzing the ad-hoc installation of surveillance cameras at ATM cubicles to identify any threat to ATM PIN security.
- Identify the potential to discover the ATM PIN through visual analysis of surveillance camera footage.
- Develop methods for identification of the PIN entering by analyzing video footage.
- Create a threat model of the ATM system to identify the threats of revealing the ATM PIN and the impact on the banking system.

1.4 Research Approach

This research has followed a mixed research approach adopting both qualitative and quantitative analysis of data. The qualitative approach was used in analyzing the existing operation of the ATM system. Thereby the procedures followed by banks for installing surveillance cameras at ATM cubicles. Hence, it has used interviews as a qualitative method. The experimental approach was employed due to the restrictions to use real surveillance camera footage of ATM cubicle for the analysis. Thus an experimental research was created to simulate the real ATM cubicle. To identify the potential of manual inference of the ATM PIN through the close observation of video of the PIN entering process, an in-person survey was conducted. Thus, the experimental approach and the survey was adopted as quantitative analysis.

The flow of the research process is presented in the Figure 5.19 below.

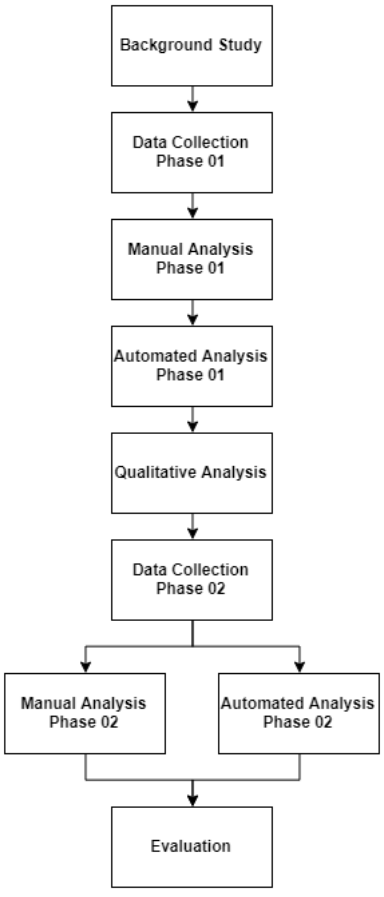

Figure 1.1: Flow of the research approach

Background Study

Comprehensive study on the research domain has been carried out based on previous literature and domain related resources.

Data collection Phase 01

As the research design, a laboratory setup was created to simulate the PIN entering process of an ATM in order to reproduce the threat scenario. Sample videos of the PIN entering process was recorded using the laboratory setup for the analysis. In the PIN entering process of data collection, PIN pad designed with arbitrary dimensions has been used.

Manual Analysis Phase 01

A survey was conducted to identify whether the PIN can be inferred by observing the surveillance camera footage of the PIN entering process through the human naked eye. Manual Analysis Phase 01 used the sample videos captured in the Data collection Phase 01.

Automated Analysis Phase 01

A marker was place on the forearm of the user who is entering the PIN. This marker based detection and tracking of the forearm analyzed to infer the PIN.

Qualitative Analysis

A qualitative analysis was conducted by interviewing personnel from different state and private banks of Sri Lanka and resource persons from related domains.

Data Collection Phase 02

Based on the insights gathered in aforementioned qualitative analysis, the PIN pad prototype was revised to meet the actual dimensions of an ATM PIN pad. Accordingly, PIN pad was designed as per the standard Large PIN pad model (JUST E6021) which is commonly use in Sri Lanka (personal communication, 2019). Sample videos of the PIN entering process were recorded using this PIN pad in the laboratory setup.

Manual Analysis Phase 02

A survey was conducted using the sample videos of the PIN entering process captured in Data collection Phase 02.

Automated Analysis Phase 02

An OpenCV python programme was created to extract the key presses by marker based tracking of the forearm. A java programme was created to guess the PIN in video footage which uses the coordinates of the forearm movements.

Evaluation

Evaluation of the results derived from Manual Analysis Phase 01, Manual Analysis Phase 02 and automated analysis were evaluated against the ground truth. This ground truth will also be referred to actual PIN and vice versa throughout this thesis.

1.5 Limitations, Scope and Assumptions

1.5.1 Limitations

The access to real surveillance camera footage of ATM cubicles is restricted by the law and is only provided to lawful bodies and on a formal subpoena or court order (personal communication, 2019). Therefore, this research used sample videos which were captured utilizing the laboratory setup which was designed to stimulate the real ATM cubicle.

1.5.2 Scope

In scope

The below aspects will be maintained when performing the research.

- This research focus one individual rather than a group of individuals for the PIN guessing process which narrow down the scope of the research.
- The research will not consider real-time ATM surveillance camera footage videos for the manual and automated PIN inference process. However during the background study, real-time surveillance camera footage of ATM cubicle were observed.
- Marker-based hand tracking was used to detect and track the hand movements.

Out scope

- This research is only focused on showing the potential of inferring the ATM PIN and security implications to the banking system due to the exposure of

the PIN. The possible attacks which resulted after the PIN exposure will not not be considered.

1.5.3 Assumption

The research is performed on the basis of the following assumption

- The PIN can be inferred from surveillance camera footage of an ATM cubicle.

1.6 Contribution

This research fill an existing knowledge gap by contributing the following,

- To the best of our knowledge, this research was first to analyze the implication for ATM PIN security caused by installing surveillance cameras at ATM cubicles.
- The results of this research shows that there is a potential threat to the ATM PIN security.
- This research introduce a novel approach to infer the key presses using video footage and produce an algorithm which guesses the PIN using inferred key presses.

Chapter 2

Background

With the observation of widespread installation of surveillance cameras at ATM cubicles, a comprehensive background study was performed to discover the objective of such establishment.

A detailed study on the ATM system in Sri Lanka was performed by the researchers to identify the purposes of installing surveillance cameras at ATM cubicles and whether there are any rules, regulations, guidelines and best practices followed by the banks when positioning wall-mounted surveillance cameras at ATM cubicles.

2.1 ATM system in Sri Lanka

The banking sector presents a prominent place in the financial system of Sri Lanka with 72.5 percent of the total assets of the financial system at the end of 2018 [7]. It comprises 26 Licensed Commercial Banks (LCBs) and 7 Licenced Specialised banks (LSBs). The banking sector of Sri Lanka continues to promote economic growth and development whilst improving banking services to its customers.

The banking sector in facilitated diverse payment services for the customers to carry out financial transactions. According to CBSL, non-cash payments can be performed with Real-Time Gross Settlement (RTGS) System and Retail Payment Systems and Instruments [8]. ATM is one of the payment card infrastructures which is under Retail Payment Systems and Instruments offered by the financial system of Sri Lanka. ATMs were introduced to Sri Lanka in 1986 and serve as a self-service banking channel. ATM is used to give a number of banking services such as cash withdrawals, balance inquiries, cheque book requisitions, fund transfers, cash, and cheque deposits, utility bill payments and change of PIN etc.

CBSL held three types of deposits of financial instruments namely demand deposits, savings deposits, fixed or time deposits. Banks allows its customers to withdraw funds of demand and savings deposits from ATMs through ATM cards and debit cards [9].

In Sri Lanka, ATMs are widespread across the country. Despite different income levels, education level, living status and occupation, people use ATMs as a convenient banking services. According to the Payments Bulletin Second Quarter 2019 issued by Payments and Settlements Department Central Bank of Sri Lanka (CBSL) [8], the number of ATM terminals in use as at the period of Quarter two 2019 is 4,930 (Provisional) and total volume and value of financial transactions during the period (cash withdrawals at ATMs during the period) is 62.5 million and 769.2 million respectively.

Description	2018	Q2 2018	Q2 2019 (a)	Percent Change Q2 18/17	Q2 19/18
1. Number of ATM terminals in use (as at end period)	4,618	4,406	4,930	9.1	11.9
2. Total volume of financial transactions during the period (million)(b)	253.8	62.5	65.8	7.2	5.2
3. Total value of financial transactions during the period (Rs. billion)(b)	2,744.8	683.5	769.2	17.9	12.5

(a) Provisional
(b) Cash withdrawals at ATMs during the period

Sources: Licensed Commercial Banks
Licensed Specialised Banks
Finance Companies

Figure 2.1: ATM usage in Sri Lanka

In general other than the ATM machine, ATM terminals consisting of Cash Deposit Machines (CDM) and/or Cash Recycler Machines (CRM) which are also allowed to make other non-cash payments. Some financial institutions provide these facilities to perform cash withdrawals, balance inquiries, utility bill payments, fund transfers, etc. through CDMs and/or CRMs, in addition to providing cash depositing facility. As per the Payments Bulletin Second Quarter 2019, the number of CDMs/CRMs has increased by 67.4 percent which indicates a number of volume of transactions also.

Description	2018	Q2 2018	Q2 2019 (a)	Percentage Change Q2 19/18
1 No. of CDMs/CRMs in use (as at end period)	1,799	1,274	2,133	67.4

(a) Provisional

Sources: Licensed Commercial Banks /Licensed Specialised Banks /Finance Companies

Figure 2.2: No of CDMs CRMs usage in Sri Lanka

Hence, ATM is one of the baking systems where there are a large number of volumes and values of the ATM transaction takes place. This has magnified the concern towards the security aspect of ATMs. Accordingly, it can be identified that the majority of the ATM cubicles are equipped with surveillance camera system as a physical control to monitor the environment inside the ATM cubicle for any unusual incidents or events that might happen.

Therefore, in order to gain a comprehensive understanding regarding the installation of surveillance cameras at ATM cubicles, researchers reviewed

and analyzed policies, guidelines and regulations imposed by both local and international regulatory bodies for installation of surveillance cameras at ATM cubicles and held few interviews with three banks of Sri Lanka.

2.2 Policies, guidelines and regulations for installation of surveillance cameras at ATM cubicles

2.2.1 Policies, Guidelines And Regulations by Local regulatory bodies

CBSL is the monetary authority of Sri Lanka who is responsible for regulating and supervising banks and selected non-bank financial institutions by the Banking Act and the Monetary Law Act. Providing settlement facilities and regulation of payment systems is one of the core functions of CBSL [10]. Accordingly, the regulation and supervision of the activities by the service providers of payment cards and mobile phone-based payment systems are controlled by the Service Providers of Payment Card Regulations No. 1 of 2009 which was issued in July 2009. This regulation was then replaced by the Payment Cards and Mobile Payment Systems Regulations No. 1 of 2013 (Regulations) on 07 June 2013. Under this regulation, the issuers of payment cards and financial acquirers of payment cards need to obtain licenses from CBSL to involve in the business or function as service providers of payment cards.

When reviewing acts, directions, circulars, and guidelines issued by CBSL, it was identified that there are only a few of them which have specifically addressed the security aspect of ATMs and relating to the video surveillance system at ATMs. According to Payment and Settlement Systems Act, No. 28 of 2005, Regulation number 18 [11], it has stated that CBSL without prejudice may issue directions, directives, rules, conditions, circulars, guidelines or instructions to any one or more Licensed Service Providers concerning the approach in which Licensed Service Provider need to conduct the business activities. Here, CBSL has considered the security features of technology relating to payment cards or mobile payment systems. With regard to the security of ATMs up until now, CBSL has published two circulars to all financial institutions facilitating electronic payments instruments or mechanisms. One is discussing to provide real-time notification for all the transactions effected through ATMs with the consent of the customers [12] and another circular is addressing to establish relevant security features as precautionary measures and to educate the customers regarding the safety of their electronic transaction to avert from any fraudulent activity at ATMs [13].

This is the only circular which was discovered that discusses surveillance cameras at ATMs. Accordingly, it has issued addressing all licence banks of Sri Lanka recommending the installation of CCTV cameras to enhance surveillance at ATM cubicles. However, this circular does not provide any recommendations on the positioning of the camera(s) in ATM cubicles.

Therefore, it was identified that it is the sole responsibility of individual banks in Sri Lanka to maintain necessary policies and guidelines to address the right procedures for installing ATM CCTV cameras (personal communication,2019). Hence, the researcher conducted interviews with three banks of Sri Lanka to explore and analyze the policies and guidelines that individual banks follow when installing surveillance cameras at ATM cubicles which have presented in detail in section 2.3.

2.2.2 Policies, Guidelines And Regulations by International regulatory bodies

When analyzing the international policies, guideline and regulations relating to the installation of surveillance cameras at ATM cubicles, PCI compliance standards were found to be greater emphasis addressing this aspect. PCI compliance standards are referred to the technical and operational requirements imposed by the PCI Security Standards Council that must be followed to secure and protect ATM/debit/credit card data of the cardholders and transmitted over the card processing transactions. Furthermore, in accordance with the Baseline Security Standards for Information Security Management [14] by CBSL, it has stated that an organization needs to comply with the PCI DSS standard in order to be recognized as a competent online or e-banking service provider.

According to PCI, PCI PTS POI ATM Security Guidelines [1] provides security guidelines and best practices to mitigate the attacks aimed at compromising the security sensitive information such as PIN and account data at ATMs. This considers both the hardware and software aspects. Hence, the primary objective is the alleviation of magnetic-stripe or equivalent image data-skimming and PIN stealing attacks at ATMs or other ATM manipulation to theft cardholder information. PCI PTS POI ATM Security Guidelines has developed by obliging ATMIA/GASA, European Payment Council, Microsoft, Trusted Security Solutions, NIST, and other PCI standards. Yet, these ATM Security Guidelines are not designed to provide any security guidelines and requirements which are mandatory by law for security certification of ATMs. As per PCI ATM Security Guidelines, the PIN entry is considered as a significant aspect of an ATM's architecture and usage that intensifies the concern of criminals. PCI ATM Security Guidelines encourage the installation of surveillance cameras at ATM cubicles in situations where possible and allowed by law. However, the Guidelines and Best

Practices of PCI ATM Security Guidelines state that the location of the surveillance camera installation needs to be carefully identified to ensure that the images of keypad entry are not captured. The surveillance camera needs to be installed to assist the attachment of alien devices to ATM front and possess the capability to produce an alert for remote monitoring if the camera is blocked or otherwise disabled.

2.3 Interview with the three banks of Sri Lanka

The interviews with the three banks were conducted with a view to observe the compliance of policies, guidelines and regulations imposed by local and international regulatory bodies in the ATM system.

During the interviews, it was found that the banks in Sri Lanka install surveillance cameras at ATM cubicles to satisfy two main requirements. The first requirement is to monitor and capture the face of the person who is entering the ATM cubicle. The second requirement is to focus on the cash dispensing area of the ATM machine. However, not all the ATM cubicles are equipped with wall mounted surveillance cameras and there are some ATM cubicles set up with two surveillance cameras.

Furthermore, the researchers were able to inspect the ATM cubicles and also to view the real video streams on screens at the surveillance control rooms. During this inspection, it was identified that there are incidents where the PIN pad is visible fully or partially when a customer is entering the PIN due to the ad-hoc installations of surveillance cameras at ATM cubicles. This revealed that the current practices of installing surveillance cameras do not comply with the PCI PTS POI ATM Security Guidelines.

Further analyzing this issue in the ATM system, during the interviews it was studied the policies, guidelines and regulations followed by individual banks when setting up ATM surveillance cameras.

2.3.1 Overview of the three interview

Each discussion with the banks was conducted with a set of questions prepared prior to the interviews (See Appendix A).

Note: The three banks are referred to as Bank A, Bank B and Bank C throughout this thesis.

Details of the information identified regarding each bank during the interviews are summarized and presented in Figure 2.3. **??**[1] [2].

[1] In CRMs, the camera placed straight focusing on the cash dispense areas right above.

[2] However, the position of the camera(s) to be placed will depend on the agreement and the

Description		Bank A	Bank B	Bank C
Date(s) of the interview	Interview 1	24/10/2019	04/11/2019	05/11/2019
	Interview 2		06/11/2019	
No of participants		3	6	4
Number of ATMs owned by the company		310	730 (Total of 1141 ATMs, CDMs and CRMs)	853
Details of the vendors to install ATMs (Separate vendor or in-house development)	ATM cubicle	Separate vendor	Separate vendor	In-house development
	Video surveillance system	Separate vendor (Call Lanka Telecom (Pvt) Ltd)	Separate vendor	In-house development
Type of camera use		IP cameras (motion to zoom cameras)		Analog cameras (motion to zoom cameras)[1]
Observe real surveillance video stream		Yes	No	Yes
	Full or partial visibility of the PIN pad	Yes	During the interview, it was revealed that it can observe the PIN pad	Yes
Any policies or guideline followed by the bank in the process of establishing ATMs and video surveillance system		Have particular specifications and policies	No specific policies or guidelines (minor feasibility study is conducted with a new ATM installation)	Consider the distance and height, the location and the size of the ATM cubicle
Requirements when installing surveillance cameras at ATM		Focus on the door entrance and cash dispense area	Focus on the door entrance and cash dispense area,[2]	Focus on the door entrance and cash dispense area
Monitoring of video footages (central monitoring or branch level monitoring)		Both central monitoring from 7.00 p.m to 6 a.m and branch level monitoring	Branch level monitoring only with 3 months backups	Both central monitoring and branch level monitoring
Access to video footages		Security division for central monitoring and branch manager in branch level monitoring	Branch manager in branch level monitoring and higher authorities of the bank.	Security division for central monitoring and branch manager in branch level monitoring

Figure 2.3: Summary of Bank Interviews

supervision of the authorized person as regards the situation

2.4 ATM PIN security

In the context of financial transaction, PIN is considered as key to is required in authentication process of a user accessing a system. In the process of authenticating, the user needs to provide a user identification token (the user ID) and the PIN to gain access to the system. PIN is unique for each user and the user is granted access to the system only when the PIN entered matches with the PIN stored in the system.

In the banking system, ATM PIN with a debit card or credit card is used in the banking system for the authentication of ATM in order to perform an ATM transaction. Hence it is a mechanism to verify the user to proceed with the transaction.

PIN is considered as a piece of confidential customer information as it grants access to important services such as financial transactions. Therefore, banks make very large investments and use a payment Hardware Security Module (HSM) for PIN generation, management and validation. The main purpose to employ a payment HSM is to advance a high level of protection for user PINs, hence to ensure confidentiality.

Therefore, it is important to protect the PIN as it authorized the access to sensitive information.

2.4.1 HSM and ATM system

An interview with a technical expert of ATM system information technology and services industry (Dr. Chaminda Ranasinghe,personal communication, 2019) was performed to gain a deeper understanding of how HSM and ATM system operates.

The details of this process which was identified is present below. HSM is a part of the ATM system which is employed for the ATM PIN management validation process. It is known as the military-grade security module. The Local Master Key(LMK) is the main key which is used to arm the HSM and is composed as key parts. It requires an integration of all these key parts and to generate the LMK to arm the HSM.

When considering the use of HSM in the ATM system, all the user PINs are stored in the HSM. In general, there are two ways for a user to create a PIN. One is the random PIN generated by the HSM (Print Mailer) and the other way is that the user creates his own PIN via ATM. Either way the PIN offset[3] is securely stored in this HSM.

In the authentication process of the ATM system, when the user enters the

[3]PIN offset is the reference key to the PIN block which is stored in the client information database whereas PIN block is the encrypted PIN which is stored in the HSM

PIN, it verifies the validity of the PIN by matching the PIN Block together with the relevant PIN offset and HSM.

With this mechanism, the user PINs are protected and stored securely to ensure confidentiality, integrity and availability.

Although the banks use HSM for secure management of user PINs, it was discovered during the interviews with the three banks that the PIN entering process is captured in the surveillance camera footage at the ATM cubicle. Yet, the existing ATM system does not capture this problem that may cause a threat to ATM PIN security. Hence, the existing ATM system does not consider the surveillance camera system as a part of the system.

Therefore, a threat model was developed for the existing ATM system elaborating current practices and trust assumptions to showcase this problem after analysing the information collected during the above mentioned interviews with the three banks and technical expert of ATM system information technology and services industry.

2.5 Threat Model

2.5.1 Introduction to Threat model

Threat modeling is a method used to build an abstraction of the system which showcase the potential attackers and threats to that system [15]. It consists of assumptions with what adversary could do in order to attack an information system. Based on the assumptions of the threat model, the relevant measurements and mechanisms are implemented to ensure the security of a system. An event that breaks any of these assumptions with respect to a particular system will be resulting in an insecure state of that system. Hence, the threat mode is used to determine, communicate, and know the threats and mitigations within the context of protecting the assets of an system.

2.5.2 Threat model for the existing ATM system

The threat model which was developed for the exisiting ATM system is presented in Figure 2.4.

The existing ATM system operates under the assumption that the ATM PIN is secured and the system ensures the confidentiality of the PIN. As shown in Figure x.x, the whole banking system functions in a Trust Boundary. However, the ATM cubicle operates in an untrusted environment, yet securely controlled by the banks. ATM cubicles are in an untrusted environment because the ATM is a publically open interface. Therefore,banks protect this ATM cubicle which

operates in the untrust environment by encrypting the communication channel between ATM switch in the trusted boundary and the ATM cubicle in the untrusted boundary as a security control.

The basic trust assumption in the existing ATM system is that PIN is securely stored and is not revealed even to the internal employees who are in the trusted boundary [16].

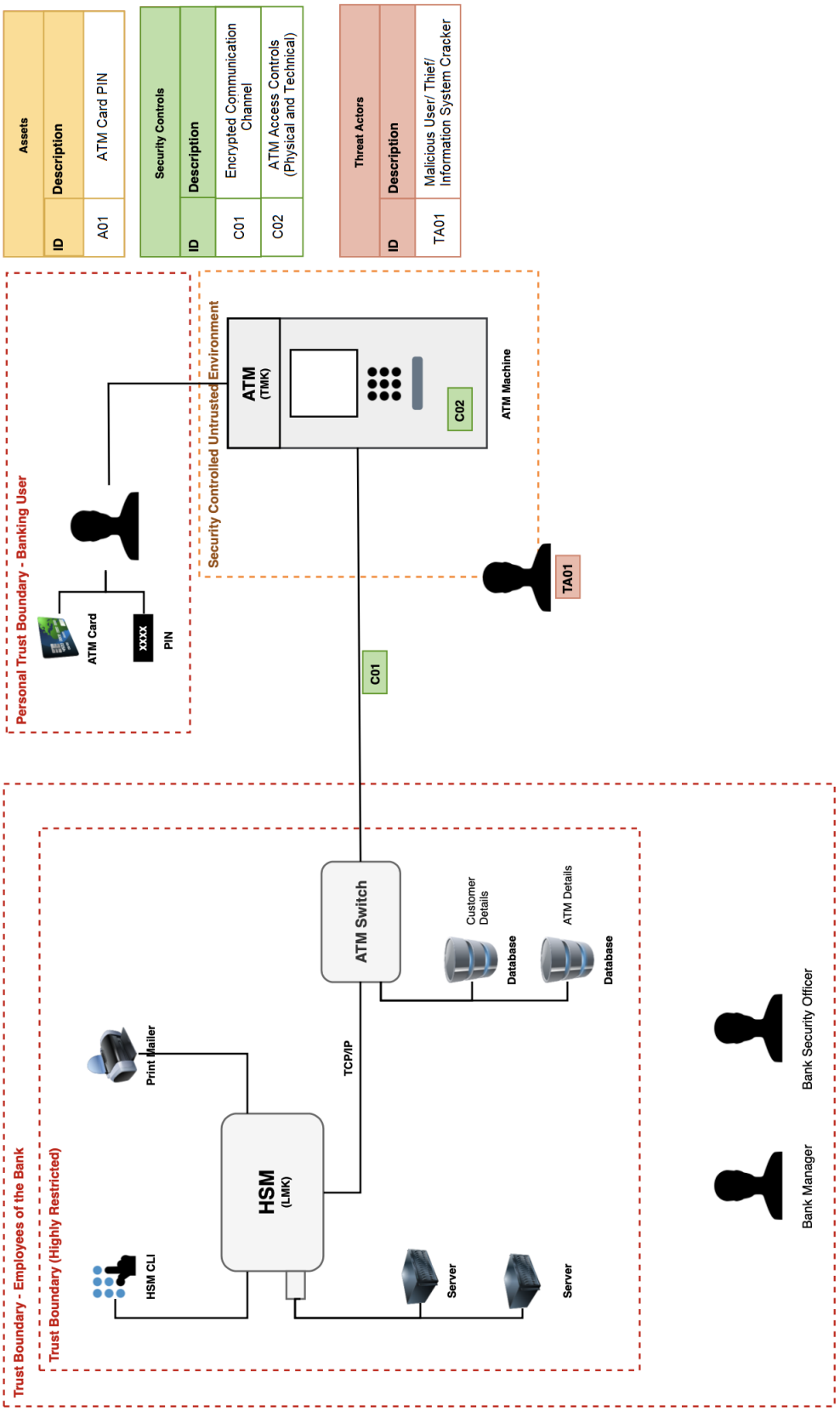

Figure 2.4: Threat model for the exisiting ATM system

Chapter 3

Literature Review

In this chapter, the recent studies of related work on this research are presented. These related studies have been reviewed based on two approaches.

1. Research regarding concerns of the security aspect of surveillance cameras
2. Inferring keyboard inputs using camera footage.

3.1 Security aspect of surveillance camera

In the research paper by Andrei Costin [17], it has conducted a systematic review of existing and novel threats and vulnerabilities in video surveillance, CCTV and IP-camera systems based on publicly available data in order to identify security and privacy risks associated with the development and deployment of these systems. The paper also presents a set of recommendations and mitigations to enhance the security and privacy aspects of video surveillance systems.

Longfei et al [18] in their paper provide a detailed study on camera-related vulnerabilities in Android phones for mobile multimedia applications with a survey and an analysis of the threats and benefits of spy cameras. It also proposes an effective defense scheme to secure a smartphone from all these spy camera attacks.

In addition, Brialogn and Zhuang [19] have tested GeoVision GV-FD220D 2MP H.264 IR fixed IP Dome camera to identify security vulnerabilities of IP cameras. According to the study, it has detected two entry points to the camera system which is accessible through Windows Explorer or the GeoVision DMMultiView client, to crack the password and to exploit the control of the IP camera. Also, Michael et al. [20] address vulnerabilities associated with Wi-Fi IP based CCTV systems. The authors have considered the relevant vulnerabilities and significant based on confidentiality, integrity, availability and present a framework which can be utilized to minimize the security risks associated.

3.2 Inferring keyboard inputs using camera footage

Mowery et al. [21] in their research, discuss the usage of thermal camera footage of a keypad after a user's typing session, to derive the possible keys pressed. ATM PIN is a specifically mentioned scenario of their research paper. First, the PIN recovery results from human/manual analysis has been presented. Secondly, the researchers incorporated computer vision techniques to automatically extract the code from the created heatmap of the thermal camera data. Even though the automated analysis only slightly outperformed the manual analysis it has demonstrated the potential to scale such attack scenario in practice.

Even though the Mowery's research is aligned with our main research domain, the PIN security, it requires a special thermal camera to be used after each of the subject typing the PIN using the pin pad. Even though the need of footage of a user's PIN entering process is not required in this attack scenario, a clearly visible thermal imagery of after the process is required. Since we were exploring the possibility of surveillance cameras at ATM cubicle implications of ATM PIN, the literature review has been carried forward concerning the instances where surveillance cameras have been used in such attack scenarios.

Balzarotti et al. [22] in their paper, present a tool named Clearshot which automatically constructs the most probable text from video footage of a user's keyboard typing process. The video is captured using an over the keyboard video camera with a full view of the hand and the keyboard. In constructing the process to recover the text being typed, firstly, the video recording of the typing session of the user is analyzed to identify the hand or finger movements and possible key presses. The researchers then follow an occlusion-based analysis, that is to a key to be pressed it is necessary that the key is at least partially occluded by the finger and a light-based analysis which identifies the contours of keys and then differentiate adjacent frames of the video to infer the likelihood of that key being pressed. Then these data are forwarded to a text analysis process to construct the most probable text that has been typed. As per the evaluation of this approach, it was identified that Clearshot was able to extract a substantial proportion of typed text by the user and to suggest around 80% words correctly within the first 50 choices of correct words proposed.

In the study by Maggi et al. [23] on iPhone, Android and Blackberry mobile devices on the dynamic conditions present that key magnifying feedback provided from these devices are vulnerable to shoulder-surfing attacks. Hence, there is no specific positioning of the attacking camera and the target device. The discussed attack was facilitated by computer vision and image processing techniques to

identify possible key magnifying events. This study proposed a fast method to infer keystrokes from either online or offline video(s). It concludes that the key magnification feedback is not suitable for applications which require high security.

Qinggang Yue et al. [3] have used Google glass-based spy camera attack on touch screens to decode the typed input, where the input is not visible to the naked eye. However, it needs to have a direct sightline to the fingertips of the user. The basic idea of this approach is to track the movement of the fingertip and use its relative position on the touch screen to detect the pressed keys. By applying the optical flow, deformable part-based model, k-means, and clustering and other computer vision techniques to automatically track and analyze fingertip movements. Based on this study, it was able to decode more than 90% of the typed passcodes.

The three of the aforementioned researches depicts the requirement of a direct line of sight of the keypad/ typing fingers. While in an ATM scenario a direct line of sight towards the keypad, through the surrounding surveillance cameras is not a luxury mostly, the literature was pursued furthermore to explore what other aspects of such attack scenarios have taken place.

As per the study by Raguram et al. [5], it presents an exploitation on mobile device keyboards by analyzing key pop up events through direct and indirect surveillance of the instant. Without limiting the direct line of vision towards the keyboard, indirect sight channels such as reflections from sunglasses were used as the medium of surveillance. Either from direct or indirect line of vision, a classifier was trained to identify the key popup event. And thus, using this classifier the key popup event has been identified and the most probable input has been inferred. It has used advanced computer vision algorithms to construct the typed input. It was found that more than 35% of their hypotheses achieved a perfect score.

Xu et al. [4] in their study, propose a method to automatically reconstruct user typed inputs from compromising reflections. This approach is most related to the approach that is discovered by Maggi et al. [23] and Raguram et al. [5]. However, the methods operate on small and/or high noisy video images. But in this study, it automates the reconstruction of typed input on mobile devices using advanced computer vision and image recognition techniques. Despite using the key pop-up event to exploit the threat, it has employed a fingertip motion analysis technique to track possible key presses and broaden the applicable keyboard types. Comparatively less-expensive camcorders were used to capture videos. It 10 was able to reconstruct typed input within a 3m-50m range with this method. This study presents that there is a considerable threat to information security by such attacks.

While Raguram et al. uses the key pop up event of smartphone keyboards from

a reflecting surface, combined with a trained classifier, Xu et al. has identified the fingertip movement of the footage from a reflecting surface to construct the typed input. Both of these studies do not require a direct line of vision, but some visibility of the keyboard or the fingertips itself is required.

Jin et al. [24] present a novel vision-based attack towards keyboard inputs. In this study, it has created a tool called ViviSnoop which uses camera footage of a typing session to construct the typed phrase by analyzing the subtle vibrations of the desk, where the keyboard is placed, which occurs with each key press. It emphasizes the fact that even using ordinary surveillance cameras, keyboard inputs can be inferred unauthorized despite not having a direct sightline on the keyboard inputs.

A recent study conducted by Chen et al. [25] prototype and evaluates that gaze-based attacks exploit with a video are possible within a short distance and a small angle between the camera and the victim. In this work, it proposes a novel keystroke inference method exploited by recording the eye gaze. As per the study, it was able to infer PINs, unlock patterns and text input to mobile devices.

Both of these studies show that there is an information security threat to keyboard inputs from surveillance, even if there is no direct or indirect line of sight towards the keyboard/keypad or the user's input scenario.

In the research study by Shukla et al. [6], it was used around 200 video footage of typing the PIN using an HTC phone focusing on the rear side of the target device. It selects a point in the hand to track the movement. Depending solely on spatiotemporal dynamics of the hand during the typing process, the typed PIN is decoded. It does not depend on having a direct line of sight to the keypad of the target device. From this study, it has shown that it was possible to infer 50% PINs in the first attempt and up to 85% accuracy in the tenth attempt.

This particular research grabbed the eyes of the researchers due to fact that in an ATM scenario, the visibility area of the placed surveillance camera inside the ATM cubicle might not able to either grasp the subtle variations of the ATM machine (as in ViviSnoop) or record the eye gaze of the subject (as in Chen et al) to possibly infer the user's PIN input. However as discussed later even though the keypad or the fingertips of the subject is occluded in surveillance footage, most of the time the user's arm is mostly visible. In Shukla's research the concept of using the movement of a point of the visible hand (palm in that research) to derive the typed input, has been paid attention by the researchers, to possibly explore the application of such concept in this research also.

Chapter 4

Methodology

4.1 Research Questions

Research questions of this research are as follows.

1. What is the potential to discover the ATM PIN through visual surveillance of CCTV video footage?

2. What are the threats of revealing the ATM PIN and what is the impact on the banking system?

4.2 Research Method

Researchers have adopted the experimental research design, in person surveys and interviews during the data collection. Hence this research is conducted employing a mixed research method.

The reasons behind the selection of the experimental research design were as follows;

1. Disclosure of real surveillance camera footage of an ATM from banks and financial institutes is forbidden by law and it can only be provided to lawful bodies and on a formal subpoena or court order. (personal communication, 2019).

2. Recording of the PIN entering process inside an ATM cubicle has legal consequences. This leads to identity theft, which is a federal crime [35].

4.3 Research Design

Considering the reason for the access to real surveillance camera footage, researchers have adapted an experimental research approach to conduct the

research. Hence, as the research design, a laboratory setup was created to simulate the PIN entering process of an ATM in order to reproduce the threat scenario.

4.3.1 Laboratory setup

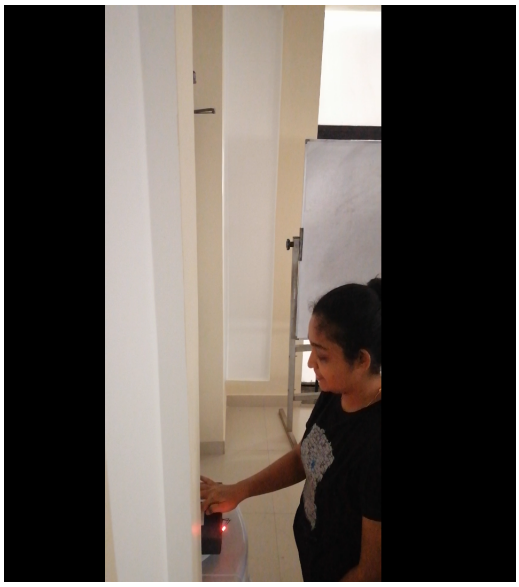

Figure 4.1: Actual Laboratory setup used

When designing the laboratory setup following conditions were taken into consideration.

1. Camera: According to the IPVM statistics, the most common resolution of cameras used in surveillance in 2018 has been. In this research, a mobile phone camera (Huawei Nova 3i [Figure 4.2], 1080p, 30fps) with similar specifications was used as an alternative to the surveillance camera mounted in the ceiling/wall in the ATM cubicle.

Figure 4.2: Phone camera used in the laboratory setup

2. PIN Pad: Two prototypes of ATM PIN pad was designed for the PIN entering the process.

   Initially, a PIN pad prototype was created according to arbitrary dimensions.

   However, following the interview with Bank C, it was able to explore different types and models of PIN pads used in ATM machines commercially. EPP7 is the latest type of ATM PIN pad to use. According to the size of the PIN pad, there are two types namely Small and Large. Figure 4.3 and Figure 4.4 are two models for small and large PIN pad respectively.

Figure 4.3: Small ATM PIN pad

Figure 4.4: Small Large ATM PIN pad

Accordingly for this research, a prototype PIN pad (Figure 4.6) was created as per the standard Large PIN pad model (JUST E6021).

Hardware implementation of the ATM PIN pad

This PIN pad was designed as an electronic keypad using 12 push buttons, 1k0/1k ohm resistor, one red LED (light-emitting diode), nine-volt battery and circuit wires. For the identification of the actual keypress event, an LED is connected to the button of the keypad. Accordingly, the LED is lighted up when each button is pressed (Figure 4.7)

Figure 4.5: Hardware components used to develop the PIN pad

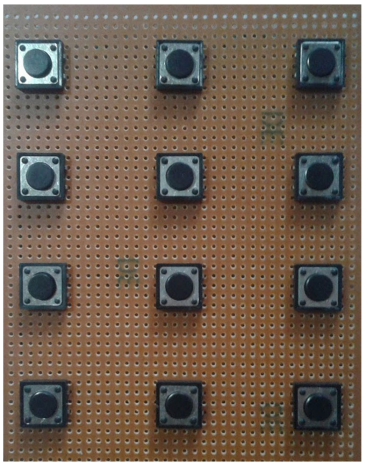

Figure 4.6: ATM PIN pad prototype design

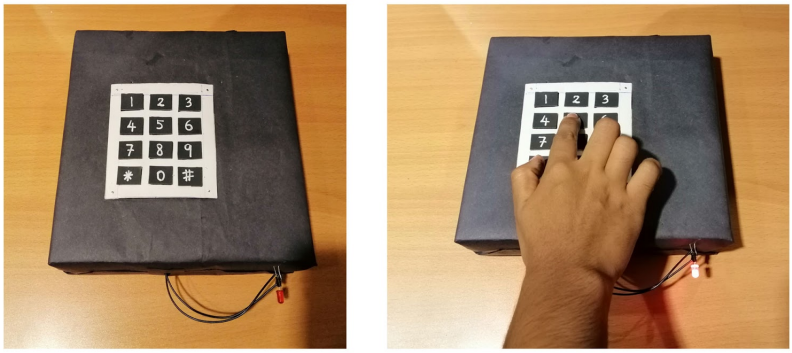

Figure 4.7: LED lighted up when a pressing a key

3. Person settings:

   (a) The user enters the PIN using the index finger of his/her right hand.

      i. It is essential to use single-finger entering because it causes the whole hand to move.

   (b) A green color sticker was placed on the upper forearm of the subject for the market-based tracking process

4.4 Data Collection

Data collection was performed in the laboratory setup which was designed simulating the real ATM cubicle.

In the data collection process, sample videos of the PIN entering process were recorded under the laboratory setup. These videos were labeled with the respective actual PIN which the subject entered.

The PINs which were used in the aforementioned data collection process were generated and selected randomly. It considered PINs with four unique digits to have clear four distinguished keypress points.

Data collection was conducted as two phases.

4.4.1 Data collection Phase 01

In the Data Collection Phase 01, the sample videos of the PIN entering process was recorded using the ATM PIN pad prototype which was created according to arbitrary dimensions.

4.4.2 Data collection Phase 02

In the Data Collection Phase 02, the sample videos of the PIN entering process was recorded using the using the standard ATM PIN pad prototype which was designed as per the standard Large PIN pad model (JUST E6021)

4.5 Data Analysis

The sample video of the PIN entering process which was gathered during the Data Collection process was analysed in two approaches as discussed below.

1. Manual Analysis
2. Automated Analysis

4.5.1 Manual Analysis

In the Manual Analysis, the sample videos of the PIN entering process were analyzed manually. This was performed to investigate whether the PIN can be inferred by observing the surveillance camera footage of that PIN entering process through the human eye (Manual identification of the PIN). Thereby to show that the ATM PIN can be exposed by the clear examination of surveillance camera footage manually.

For this purpose a survey (in-person survey) was conducted as two phases. The survey was performed with voluntary participation of undergraduates of the University of Colombo School of Computing(UCSC)

Ten video samples of the PIN entering process which was selected randomly from the sample videos of the data collection process was used in the survey. In both Phase 01 and Phase 02, the videos of these same 10 PINs were used. Table 4.1 contains the ten PINs which were contained in each video of the PIN entering process used for the Manual Analysis survey.

PIN number	PIN
PIN 1	1789
PIN 2	2650
PIN 3	5492
PIN 4	6831
PIN 5	7153
PIN 6	9416
PIN 7	5476
PIN 8	1920
PIN 9	163
PIN 10	3592

Table 4.1: PIN used for Manual Analysis

For each participant, ten video samples of the PIN entering process without the PIN label were put on a laptop computer display. The participant was instructed to observe the forearm movement of the person who is typing the PIN of that video and to guess and derive the possible keypress(es). It was instructed to guess any number of digits of the PIN even if the whole four-digit PIN cannot be identified. Participants were provided with three attempts to watch the video and to guess the PIN. A survey paper (see Appendix B.1 and B.2) was given to each participant to write down the corresponding digit(s) guessed corresponding to each attempt. In this survey paper, all the instructions were stated on how to follow through the manual analysis with an image of an ATM PIN pad for the reference.

Manual Analysis Phase 01

In the Manual Analysis Phase 01, the survey was conducted using the sample videos of the PIN entering process collected in the Data Collection Phase 01. This was conducted during the month of July, 2019.

Manual Analysis Phase 02

Sample videos of the PIN entering process collected in the Data Collection Phase 02 was used in the survey of Manual Analysis Phase 02 and was held in the month of November, 2019.

4.5.2 Automated Analysis

Automated PIN guessing application was developed with OpenCV python implementation to guess the PIN entered in each footage collected using the laboratory setup. OpenCV was used to operate on video footage of PIN entering process and python was selected due to the simplicity and availability of many

libraries to easily handle mathematical functions; Numpy, operate on datasets; Pandas and plot graphs to visualize data; matplotlib.

This Application detects and tracks the hand movement and identifies the keypress events and possible PIN combinations. The automated PIN guessing process has four steps. In **Step 1: Align Frames:** video frames are rotated to align the keypad with the OpenCV x,y coordinate system. **Step 2: Marker Based Hand Detection And Tracking:** get the position of the marker in each video frame. In **Step 3: KeyPress Detection:** keypress events are identified and in **Step 4:Pin Extraction:** guesses the possible PINs for each PIN entering process footage.

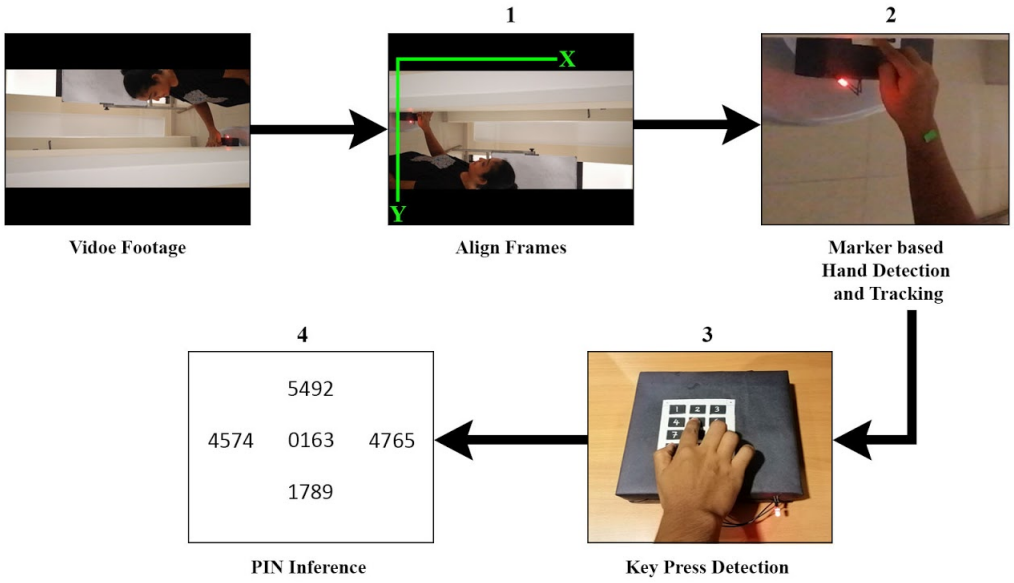

Figure 4.8: Automated analysis flow diagram

Step 1: Align Frames

Depending on the orientation of the device during the recording of the PIN entering process, OpenCV reads the video frames in different orientations. Figure 4.9 shows the actual orientation of the video while recording and Figure 4.10 shows the output when reading the exact same video using OpenCV. Even though the PIN pad is not visible in the footage the orientation of the PIN pad needs to be aligned with the X-axis and the Y-axis of the OpenCV coordinate system to make it easy to map the forearm movements. Figure 4.11 and Figure 4.12 shows the roughly estimated orientation of the PIN pad in with respect to 4.9 and 4.10.

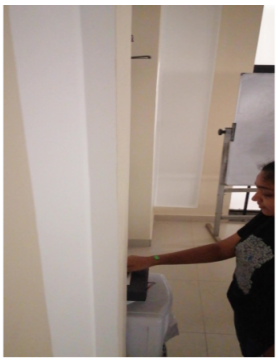

Figure 4.9: Capturing the orientation of the PIN entering process (B)

Figure 4.10: Reading orientation of the footage (B)

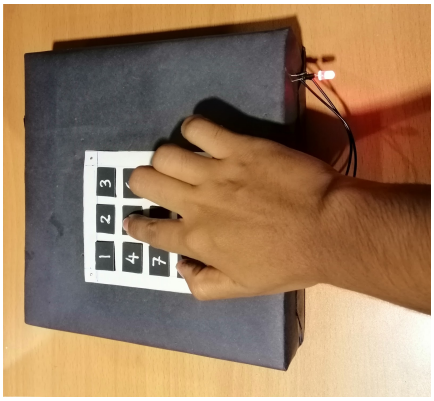

Figure 4.11: Orientation of the PIN pad A

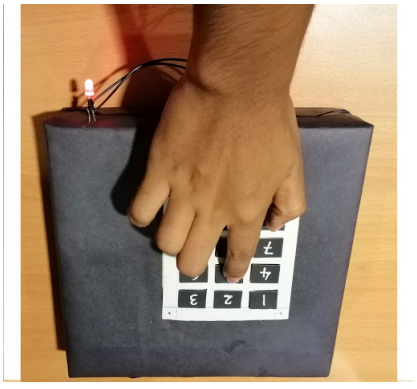

Figure 4.12: Oreintation of the PIN pad B

However, 4.13 shows the X, Y coordinate system of OpenCV which is diverges from the cartesian plane (positive points) that is used in general mathematics. We rotate each frame in the video in a way that rows of the PIN pad align in the X direction and columns of the PIN pad align in the Y direction. Therefore increment in X direction and increment in Y direction corresponds to increment in the number values on the PIN pad on the grounds. Ultimately it is straightforward to map the direction of the hand movements to the PIN patterns. After this rotation number '1' in the PIN pad positioned at the lowest X coordinate and Y coordinate while '' sign positioned at the highest as shown in Figure 4.14.

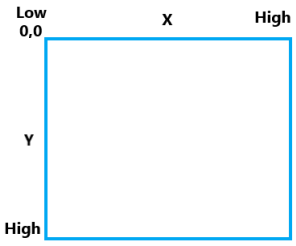

Figure 4.13: X, Y coordinate system in OpenCV

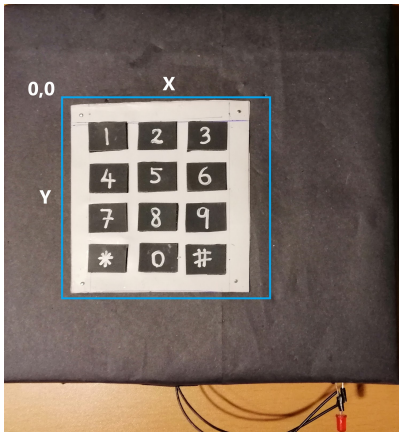

Figure 4.14: Orientation of PIN pad after alignment

Step 2: Marker Based Hand Detection and Tracking

In the process of forearm detection and tracking researchers considered two approaches. The first one is a marker-based tracking approach using colour thresholding and contour extraction and the second approach is to use a bounding box tracker with OpenCV tracking API. In the second approach, a rectangle was drawn on the forearm area to be tracked in the first frame of the video footage using the OpenCV python programme (refer appendix B.3). Then apply tracking algorithms to track the particular area. However, the bound box was deviated from the interesting area of the forearm due to background noise in the video footage.

Consequently, the resulting tracking coordinates of the hand was not sufficient to identify small movements of the forearm during the PIN entering process. In this research, as the researchers only building a proof of concept, researchers employ marker-based tracking of the hand rather than advanced hand tracking algorithms for the second approach. During the video capturing process, we put a marker which has a contrasting colour from the surroundings, on the ATM user's forearm. Researchers have developed an OpenCV python programme (refer appendix B.4) which uses colour thresholding to identify the marker in each frame. The RGB values of the marker are identified using colour picker in paint 3D and used as an input to the colour thresholding. In that programme, the RGB value of the marker is converted into HSV model for creating a mask. This mask is applied to each video frame to identify the marker in the entire video. While reading the video frame by frame, the OpenCV python programme extracts the contour of the minimum enclosing circle of the marker. Coordinates of the center of the minimum enclosing circle are recorded with respect to the frame number to trace the forearm movement during the entire video footage. Figure 4.12 shows the 3D graph of the X, Y coordinates of the forearm movement with the frame number; x-axis- the x coordinate of the center, y-axis- the y coordinate of the center, z axis-frame number.

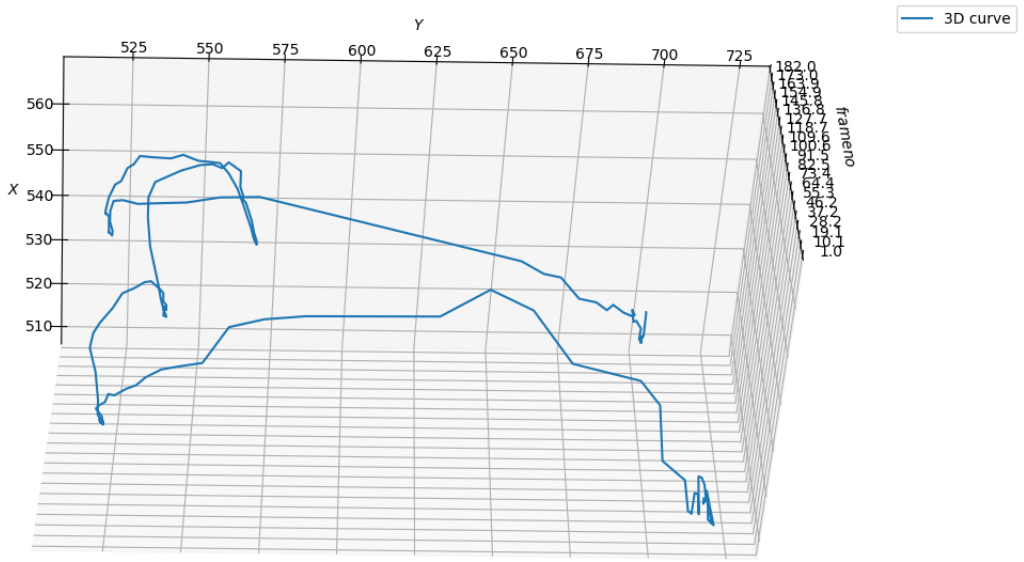

Figure 4.15: 3D Graph of forearm movement

Ground truth extraction: ssIdentification of the actual keypress events processed parallelly using the same procedure, colour thresholding and contour extraction. colour of the bulb was extracted using the same method which was used in the extraction of the colour of the marker. each frame where the bulb was blinked identified as a frame that a keypress took place. These frame numbers are

then saved for evaluation of the automated PIN guessing process.

Step 3: KeyPress Detection

Keypress events were detected using the gradient of the forearm movement. Researchers have applied a heuristic that the movement of the forearm in the X direction and the Y direction is very little compared to the movement happen when travelling between keys or no movement happens at all when ATM user is pressing a key. Researchers have confirmed this heuristic by plotting the X, Y coordinates of forearm movement and the ground truth of keypress data extracted in step 2 (figure 4.16).

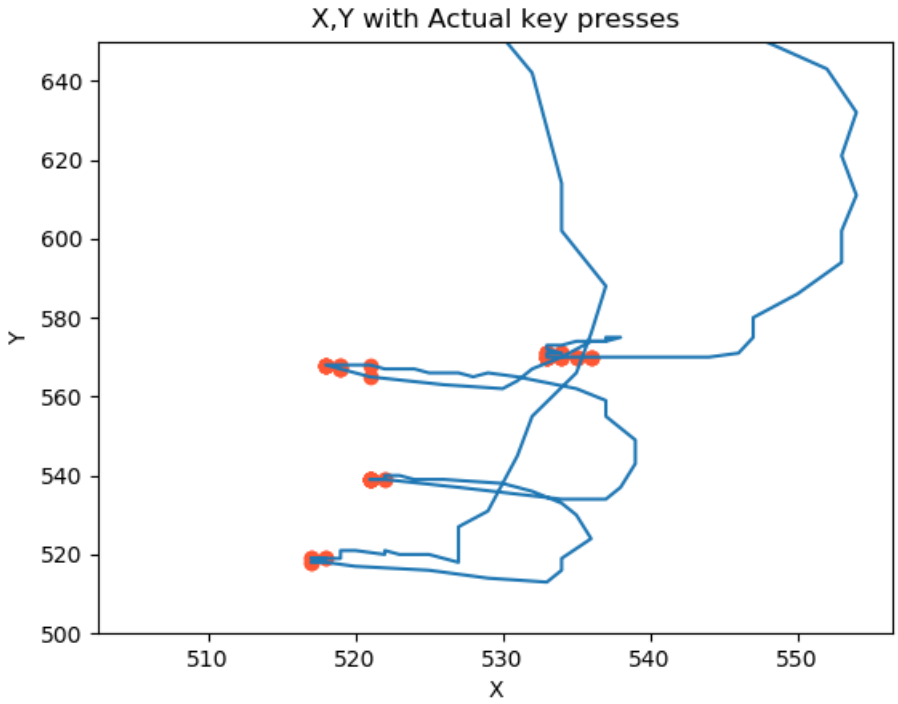

Figure 4.16: Forearm movement with actual key press

The gradient of the forearm was calculated by calculating the net gradient using gradient of the forearm movement in the X direction (dx) and gradient of the forearm movement in theY direction (dy) using the following equation(appendix calgradient).

$$\text{Net Gradient} = \sqrt{dx^2 + dy^2}$$

Figure 4.17 shows the frames corresponding to the ground truth of key presses events in orange dots on the net gradient graph of the forearm movement. it was

clear that the gradient of the keypress events was small compared to the travel between keys.

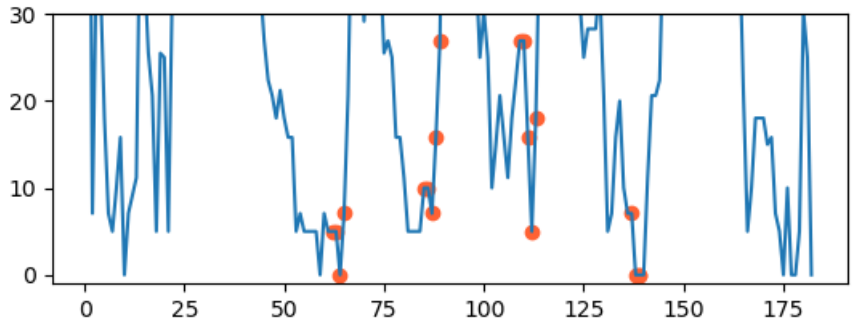

Figure 4.17: Gradient graph with actual keypress

The net gradient graph was smoothened with B-spline and median filtering to make a low pass filter and remove local valleys surrounding the keypress events. However, the smoothing resulted in affecting the valleys which corresponded to keypress because the keypress event itself is a high frequency in the net gradient graph. Therefore, the filtering process was discarded afterwards. To extract the keypress events from the net gradient data, first the local valleys of the net gradient graph were detected. for a particular frame, if the gradient of the preceding frame and the gradient of the succeeding frame is greater than its gradient the frame is identified as a valley(figure 4.18). frames preceding to the valley have a negative gradient while frames succeeding to the valley have a positive gradient.

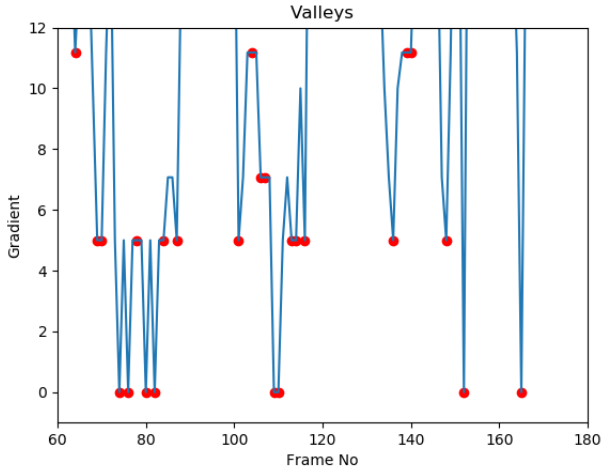

Figure 4.18: Local valleys

Through the analysis of gradient graph with the ground truth of keypresses in the above step 2, it was identified that the minimum gradient value of a frame is recorded between 0-3 when a keypress has occurred. Therefore, for each video

footage, the local valleys were identified and put a threshold of 3 to narrow down the number of local valleys. then the remaining local valleys were put into 4 clusters since there are only 04 keypresses in the PIN entering process. then the mean of the frame number calculated for each cluster. for those four frames corresponding X, Y coordinates were picked for the automated PIN guessing. Figure 4.19 shows the valleys between 0-3 used for clustering. Figure 4.20 shows the formation of the 04 clusters in 04 different colours with the mean is marked with a black dot.

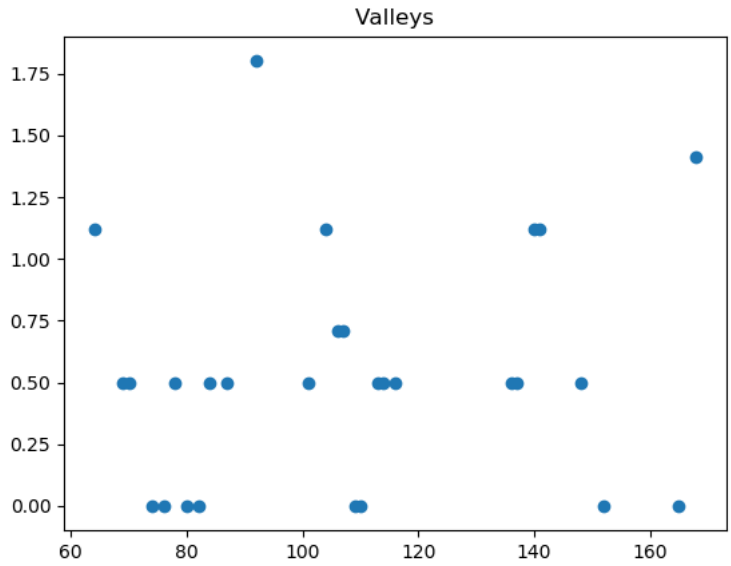

Figure 4.19: Scatter plot of valleys

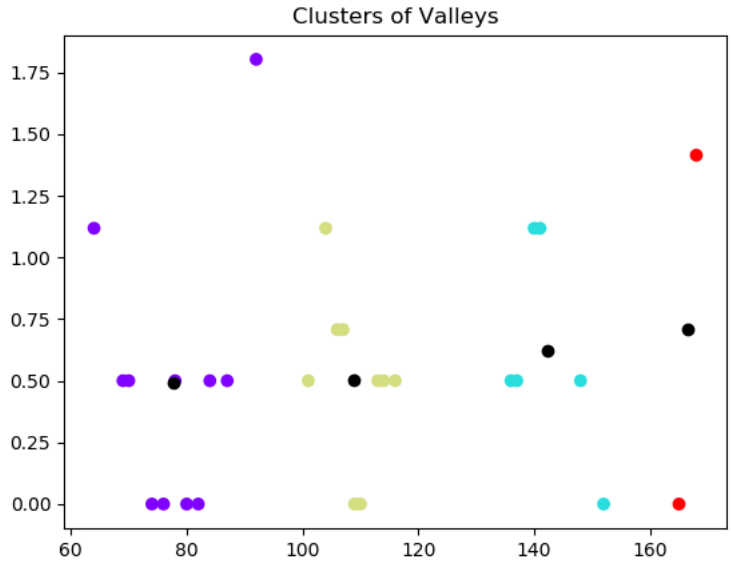

Figure 4.20: Scatter plot of valleys

Step 4: PIN Extraction

The obtained x,y coordinates of the possible 4 presses, are then used as input parameters to the PIN extraction algorithm, which will be discussed in this step.

The basic idea of this algorithm is to calculate the column row changes with regards to the previously obtained x,y coordinates. And from this data infer the possible PINs. For further clarification of this, a scenario where a user entering the PIN 2657 is taken into consideration. In the below illustration each row and column of the keypad is respectively numbered.

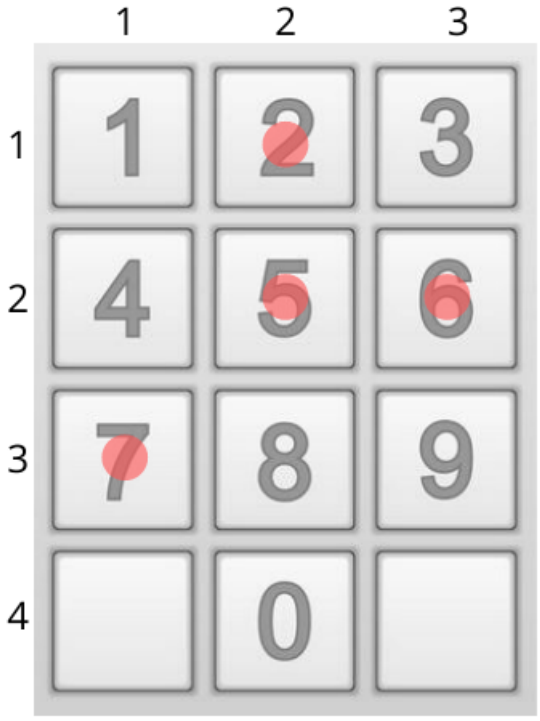

Figure 4.21: Numbered Columns and Rows of the keypad

- 2 6 ; +1 column to right , +1 row down
- 6 5; -1 column to left, 0 row changes
- 5 7; -1 column to left, +1 row down

Considering the labeled columns and rows, the changes can be summed up as +1,-1,-1 for columns and +1,0,+1 for rows.

Changes of columns:

+1,-1,-1

- Between first and second key presses, shifted one column to the right (+1)

- Between second and third key presses, shifted one column to the left (-1)
- Between third and fourth key presses, shifted one column to the left (-1)

Changes of rows:

+1,0,+1

- Between first and second key presses, shifted one row down (+1)
- Between second and third key presses, no rows shifted (0)
- Between third and fourth key presses, shifted one row down (+1)

If obtaining this data by analysing the x,y coordinates of the possible presses, it can be used to infer the Possible pin.

Following is a manual interpretation of how this data can be used to infer the PIN.

Assuming the first digit is 1.

1. The column row changes from 1st press to 2nd press is +1,+1. Which means that the next digit is one column to the right than the current column and in the next row from the current row. Which leads to the digit 5.
2. The column row changes from 2nd press to 3rd press is -1,0. Which means that the next digit is one column to the left than the current column and in the same row as the previous digit. Which leads to the digit 4.
3. The column row changes from 2nd press to 3rd press is -1,+1. Which means that the next digit is one column to the left than the current column and in the next row from the current row.

In this situation the ideal position of the expected key goes out of the scope of the keypad. Which means that the first digit is not 1.

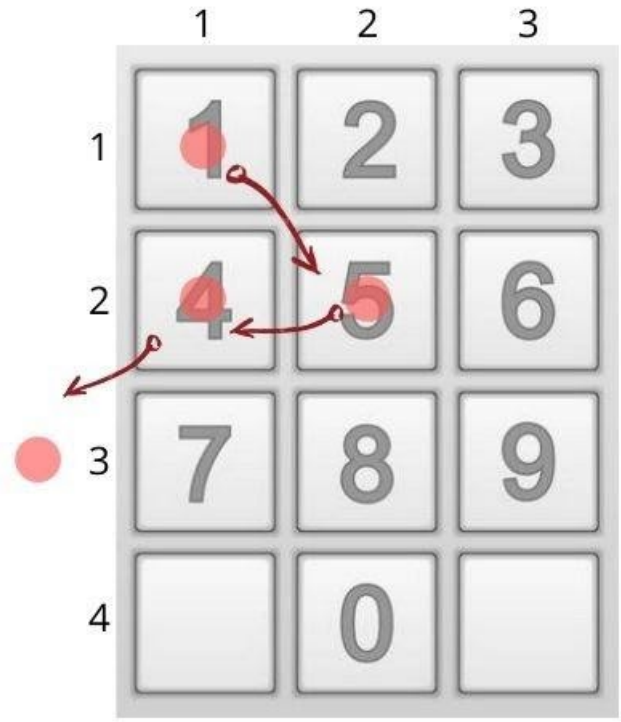

Figure 4.22: Trajectory of the presses when started from digit 1 for given change matrix

Assuming the first digit is 2.

1. The column row changes from 1st press to 2nd press is +1,+1. Which means that the next digit is one column to the right than the current column and in the next row from the current row. Which leads to the digit 6.

2. The column row changes from 2nd press to 3rd press is -1,0. Which means that the next digit is one column lower than the current column and in the same row as the previous digit. Which leads to the digit 5.

3. The column row changes from 2nd press to 3rd press is -1,+1. Which means that the next digit is one column to the left than the current column and in the next from the current row. Which leads to the digit 7.

This analysis leads to a possibly correct PIN - 2657.

Determining the column row changes using x,y coordinates

Consider the PIN 1789 and assuming the following are the sample x,y coordinates of each key pressed.

- 1 523 , 513

- 7 517 , 560
- 8 532 , 567
- 9 545 , 567

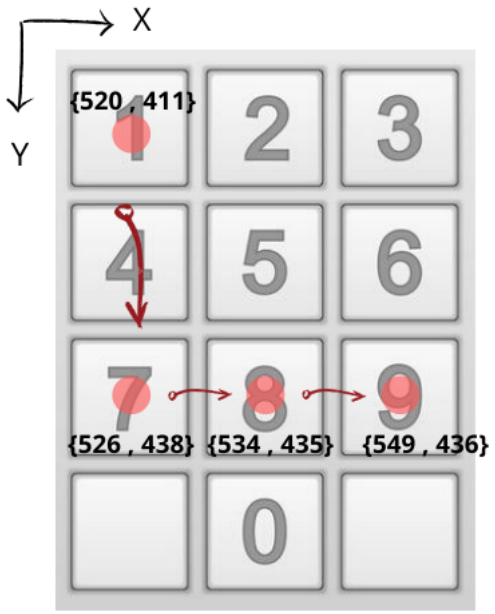

Figure 4.23: PIN 1789 trajectory

To determine the column and row changes between two presses, coordinates of adjacent digits can be deducted and get the difference. And with the difference being positive or negative, the change of column rows can be determined.

	$T_{x+1} - T_x$	Change of X	Ground Truth for actual change of columns	$T_{y+1} - T_y$	Change of Y	Ground Truth for actual change of rows
1st change	517 - 523	-6	0	560 - 513	47	2
2nd change	532 - 517	+15	+1	567 - 560	7	0
3rd change	545 - 532	+13	+1	567 - 567	0	0

Figure 4.24: Column and row changes from coordinates for 1789

In actual scenarios even for 0 change of rows or columns there could be some change of x,y can be recorded.

In the above 1st change of X there's a difference of -6 for the x axis is recorded. But the ground truth for change of X remains 0; which indicates that moving from 1 to 7 hasn't caused any change of columns, which is true.

And also if the 1st change of Y is considered, a difference of +47 for Y axis is recorded. Where the ground truth for change of Y presents 2; which indicates that moving from 1 to 7 has caused change of 2 rows. With the aforementioned, 2 main challenges were identified.

1. Identify an actual move in columns or rows.
2. Differentiate between 1 unit of change and 2 or more units of change in columns or rows.

To address these two challenges, Threshold values for both columns and rows are introduced.

- Threshold value for column - tx
- Threshold value for rows - ty

Threshold values for column and row changes

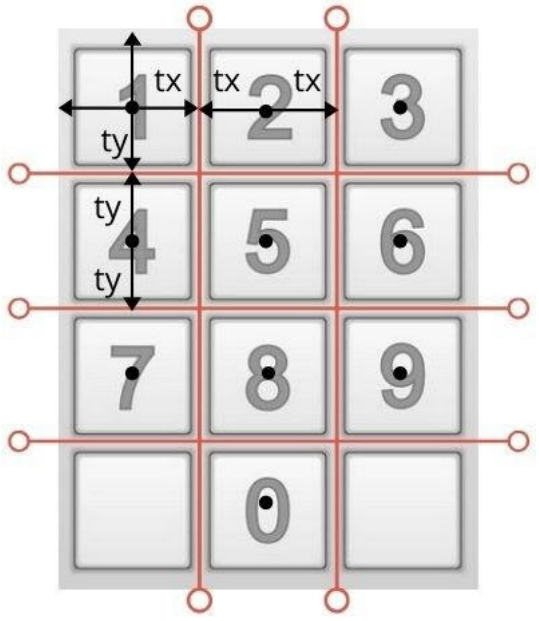

Figure 4.25: Defining a threshold value for rows and columns

If only the difference between two presses exceeds the tx or ty threshold value, it can be considered as a possible change of column or row has happened.

By comparing the difference between two presses and comparing it with the multiplication of threshold values, the change of columns or rows can be distinguished.

For each adjacent two PINs the difference of x y coordinates are calculated. Then the two functions getColumnChange getRowChange, are called for each difference having the threshold and the difference as input parameters. And these two functions will return the change of columns and rows.

```
FUNCTION getColumnChange
    Pass In: threshold, changeOfX
        IF(changeOfX <= threshold && changeOfX >= -threshold ) {
            columnChange = 0;
        } ELSE IF (changeOfX > threshold && changeOfX <= 3*threshold) {
            columnChange = 1;
        } ELSE IF (changeOfX > 3*threshold) {
            columnChange = 2;
        } ELSE IF (changeOfX < -threshold && changeOfX >= 3* -threshold) {
            columnChange = -1;
        } ELSE IF (changeOfX < 3* -threshold) {
            columnChange = -2;
        } END IF
        END IF
        END IF
        END IF
        END IF
    Pass Out: columnChange
END FUNCTION
```

Figure 4.26: getColumnChange Function – Pseudocode

```
FUNCTION getRowChange
    Pass In: threshold, changeOfY
        IF(changeOfY <= threshholdY &&  changeOfY >= -threshholdY) {
            rowChange = 0;
        } ELSE IF (changeOfY > threshholdY && changeOfY <= 3*threshholdY) {
            rowChange = 1;
        } ELSE IF (changeOfY > 3*threshholdY && changeOfY <= 5*threshholdY) {
            rowChange = 2;
        } ELSE IF (changeOfY > 5*threshholdY) {
                rowChange = 3;
        } ELSE IF (changeOfY < -threshholdY && changeOfY >= 3*-threshholdY) {
            rowChange = -1;
        } ELSE IF (changeOfY < 3* -threshholdY && changeOfY >= 5* -threshholdY) {
            rowChange = -2;
        } ELSE IF (changeOfY < 5* -threshholdY) {
            rowChange = -3;
        } END IF
        END IF
        END IF
        END IF
        END IF
        END IF
    Pass Out: rowChange
END FUNCTION
```

Figure 4.27: getRowChange Function - Pseudocode

Since the ground truths are known for the recorded PINs, different thresholds for x y could be manually tried and finally determine the most suitable threshold. However since this process is cumbersome and not very practical, a small algorithm is written to determine the most suitable thresholds using the key press coordinates of a potion of PINs gathered. And then use that x,y threshold in the main algorithm to infer the PIN.

Summary of threshold calculation algorithm

- The PINs from subject A (PINs with known ground truth and coordinates) have been used to calculate the ideal threshold
- Each PIN is labeled with its actual value and with press coordinates inferred from the previous hand tracking algorithm.

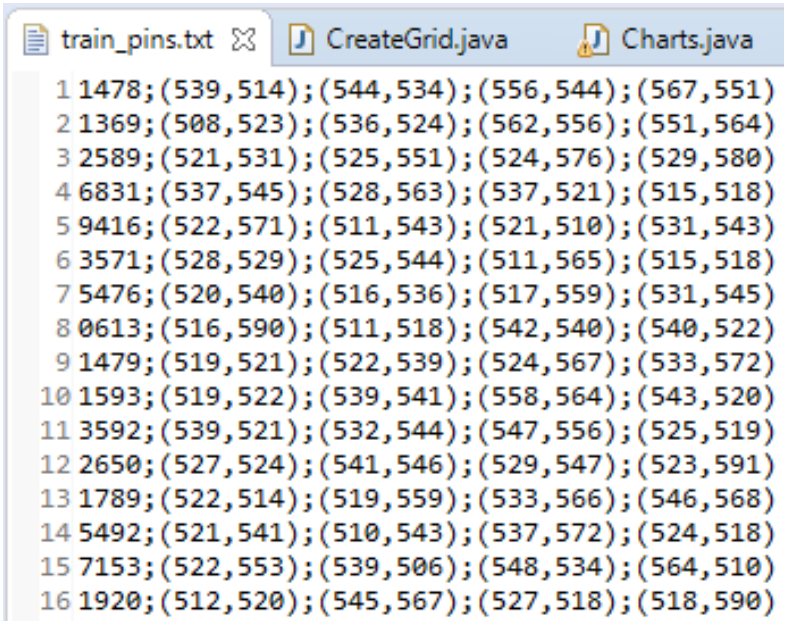

Figure 4.28: Data set used to calculate threshold values

- For both columns and rows, threshold values tx and ty are iterated from 0 to 50.
- Then each PIN is iterated through to find the coordinate difference of adjacent two presses using the above mentioned getColumnChange and getRowChange functions. Since the actual column row changes between keypresses are known at this point, the return values of the aforementioned two functions are then compared with the actual values.
- If it results in the same value, the true-counter for that specific threshold is incremented.

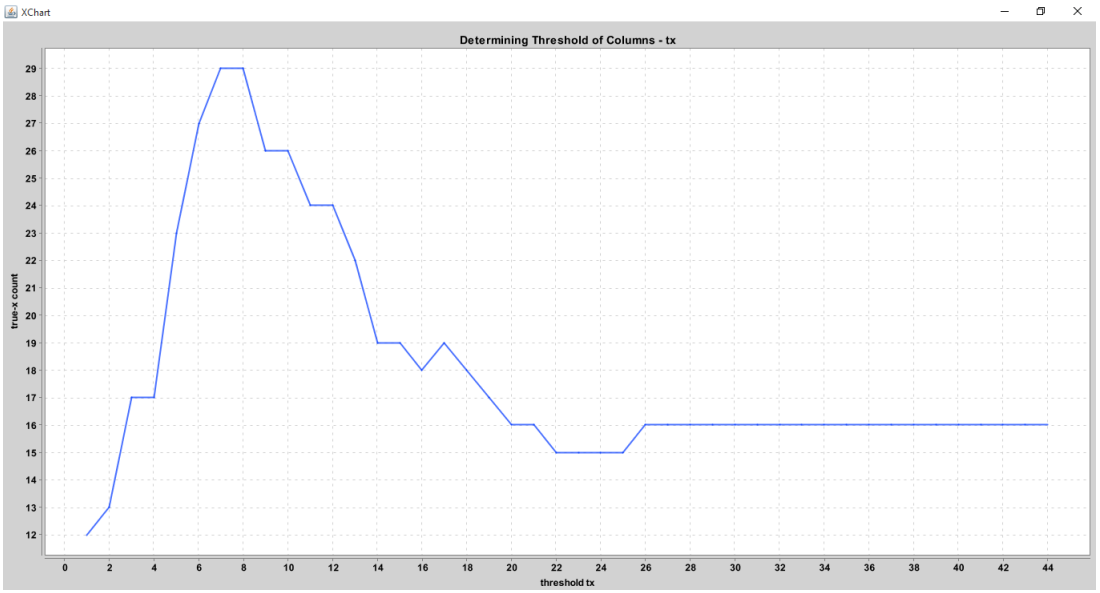

Figure 4.29: true-x count's change (correctly inferred column changes) with different thresholds

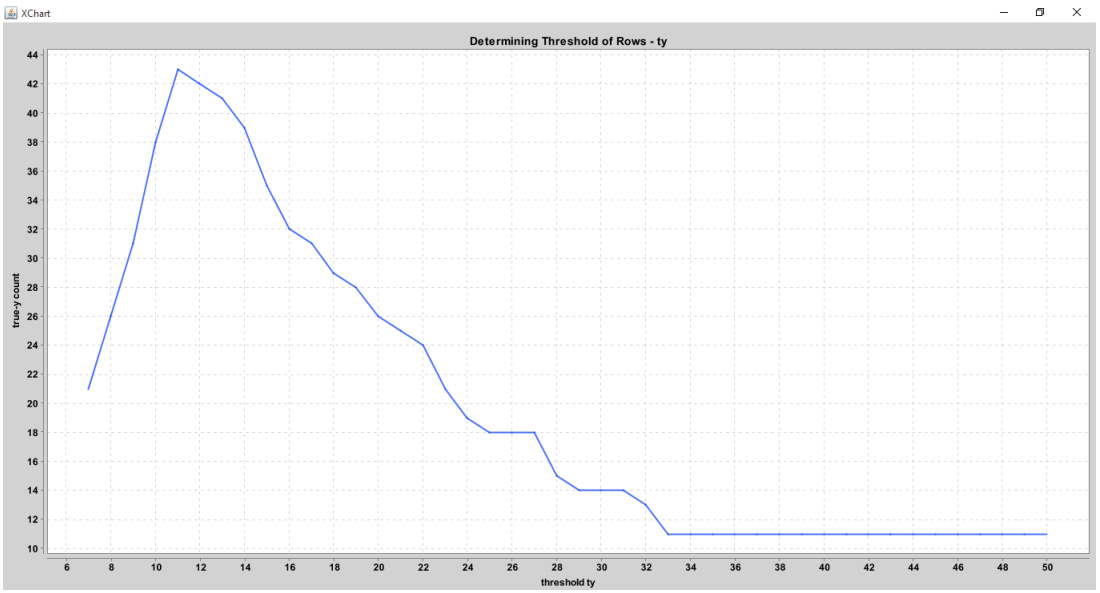

Figure 4.30: true-y count's change (correctly inferred row changes) with different thresholds

With this data set which is used to determine the optimal threshold values;

- For columns (change of X axis) tx = 7 —— 8
- For rows (change of Y axis) ty = 11

Using these threshold values (tx and ty) the aforementioned analysis based on changes between the keypresses was automated for the testing data set of subject B for X number of PINs.

Since the changes of columns rows are taken into consideration, there can be more than one matching PINs which correspond to these changes.

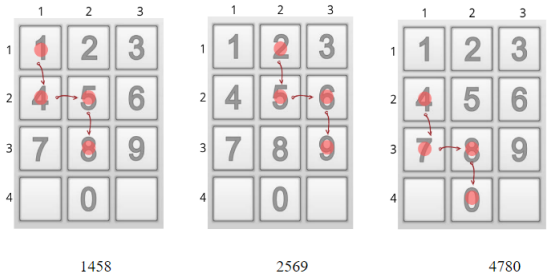

Figure 4.31: Multiple PIN possibilities for same row column changes

1458, 2569 and 4780 is such a scenario where the column row changes are identical for all the PINs; 0,+1,0 for columns and +1,0,+1 for rows.

This is somewhat a similar case that encountered in the manual analysis as well where the subjects were sometimes able to identify the trajectory of PIN but not the exact correct PIN.

In such cases to find all the corresponding PINs it is required to iterate through the whole keypad taking each key as a first key and then applying the above methodology of determining all the possibly correct PINs.

In such situations, a challenge the researchers faced was to filter out the most probable PIN in such instances.

This research is not solely focused on exactly identifying the PIN from the surveillance footage, yet shows that there's a credible threat from surveillance cameras to PIN security. However the researchers have pursued a certain path to try and filter out the most probable PIN when there are more than one suggestions from the automated analysis.

As the researchers are not tracking the subject's finger tips and since there's nor visibility of the keypad itself, mapping a virtual keypad in the video where the actual keypad is and trying to identify the subject's touch points of the keypad is a challenge. This is why in the first place the researchers adopted an approach of tracking the forearm of the subject.

With the dataset the researchers have in their hand a vague approach of clustering the X and Y coordinates of the digits has been carried out. The K-means algorithm was used in this clustering process. Since there are 3 columns and 4 rows in the keypad, 3 clusters for X coordinates and 4 clusters for Y coordinates has been derived with their cluster centroids.

- Cluster Centroids for X coordinates - 551, 569, 592
- Cluster Centroids for Y coordinates - 574 , 582 , 612, 640

And for the instances where there are more than one suggestions, the difference between actual X and Y coordinates with the corresponding cluster centroids has been calculated. And the suggested PIN with the lowest value for the difference, has been selected as the most probable PIN out of the suggested PINs.

Example -

Actual Pin	Actual coordinates (Ax, Ay)	Inferred Pins by the Algo	Cluster centroid coordinates for each digit. (Cx, Cy)	Total Deviation of actual coordinates | from the cluster centroid coordinates (|Cx - Ax| + |Cy - Ay|)
2598	(575,575), (570,595), (583,627), (564,623)	1487	(551,574), (551,582), (569,612), (551,612)	168
		2598	(569,574), (569,582), (592,612), (569,612)	106

Figure 4.32: Example calculation of difference between the calculated cluster centroids and actual coordinates of the the PIN

Out of 1487 and 2598 ; the suggested PINs from the automated algorithm, 2598 has the lowest difference with the coordinate cluster centroids, which marks it as the most probable out of two.

4.6 Evaluation

In the manual analysis and automated analysis researchers have obtained the PIN entered in each video footage. Then this inferred PINs were evaluated against the ground truth.

Chapter 5

Results and Evaluation

This chapter presents the results and evaluation of the Manual Analysis and Automated Analysis of sample videos of PIN entering process.

5.1 Manual Analysis

The Manual Analysis was conducted as described in Chapter 4 as two phases. The main consideration was to showcase whether the ATM PIN can be inferred through the naked eye of the human being by careful observation of a surveillance video of the PIN entering the process.

Manual Analysis Phase 01 and Phase 02 was performed with the voluntary participation of undergraduates of UCSC in the surveys. Each participant was given ten sample videos of the PIN entering process and three attempts to guess and identify each PIN.

The detailed results obtained in the Manual Analysis Phase 01 and Manual Analysis Phase 02 can be found in the Appendix C.1 and C.2.

The results of each phase were then explored to understand the ability of human beings on inferring the ATM PIN by observing the video of the PIN entering the process. Hence, the results were analyzed and evaluated against the relevant actual PINs to discover the following two main objectives.

- Evaluating the Manual Analysis results against the actual PIN to identify the correct PIN guessing
- Evaluating the Manual Analysis results against the trajectory of actual PIN to identify similar trajectory pattern

Following condition was taken into consideration when accepting responses of the participants for the above analysis.

- In an event of the PIN guessed by a participant contains the repetition of the same digit, then that guessed PIN was eliminated when analyzing the results.

5.1.1 Evaluating the Manual Analysis results against the actual PIN to identify the correct PIN guessing

The responses by each participant in the survey were analyzed to determine the number of digits correctly guessed with the reference to the actual PIN in each video of the PIN entering process. For each attempt, the PIN which was guessed by each participant was evaluated to discover the number of one, two, three and four (exact PIN) digits correctly identified by them. For the calculation of the accuracy of these results, the following equation has been used

$$A\,(d,n,i) = \frac{\sum_{i=1}^{n}(C_{(d,i)})}{S \times V}$$

Where Ad,n,i indicates the accuracy of correctly guessing at least d number of digits within n number of attempt(s), Cd,i is the number of correctly guessed instances with at least d number of digits in ith attempt, S and V represent the number of subjects and number of sample videos respectively.

The summary of the survey results of each phase of the Manual Analysis is presented and elaborated as follows for the evaluation of the Manual Analysis results against the actual PIN to identify the correct PIN guessing to each of the three attempts.

Manual Analysis Phase 01

1. Identification all four digits of the actual PIN (Exact PIN)

Actual PIN	No of Guessed PIN		
	1st Attempt	2nd Attempt	3rd Attempt
1789	5	5	8
2650	0	0	1
5492	0	0	2
6831	0	0	0
7153	1	4	4
9416	0	2	2
5476	3	4	7
1920	1	2	2
0163	0	0	2
3592	1	2	2

Figure 5.1: All four digits of the actual PIN – Manual Analysis Phase 01

2. Identification three digits of the actual PIN

Actual PIN	No of Guessed PIN		
	1st Attempt	2nd Attempt	3rd Attempt
1789	6	6	8
2650	0	1	1
5492	2	3	6
6831	0	0	0
7153	2	4	6
9416	2	2	2
5476	8	8	10
1920	3	4	5
0163	5	5	5
3592	1	2	2

Figure 5.2: Three digits of the actual PIN – Manual Analysis Phase 01

3. Identification two digits of the actual PIN

Actual PIN	Guessed PIN		
	1st Attempt	2nd Attempt	3rd Attempt
1789	6	6	8
2650	2	3	4
5492	4	6	8
6831	5	5	5
7153	6	8	9
9416	6	6	8
5476	8	8	10
1920	5	6	7
0163	5	7	7
3592	2	3	3

Figure 5.3: Two digits of the actual PIN – Manual Analysis Phase 01

4. Identification one digit of the actual PIN

Actual PIN	Guessed PIN		
	1st Attempt	2nd Attempt	3rd Attempt
1789	7	10	10
2650	4	6	10
5492	9	9	9
6831	7	8	8
7153	9	9	10
9416	8	8	9
5476	8	8	10
1920	9	9	9
0163	9	9	9
3592	3	5	5

Figure 5.4: One digit of the actual PIN – Manual Analysis Phase 01

The accuracy for the actual PIN identification of guessing the exact PIN, three digits, two digits and at least one digit of the PIN was calculated.

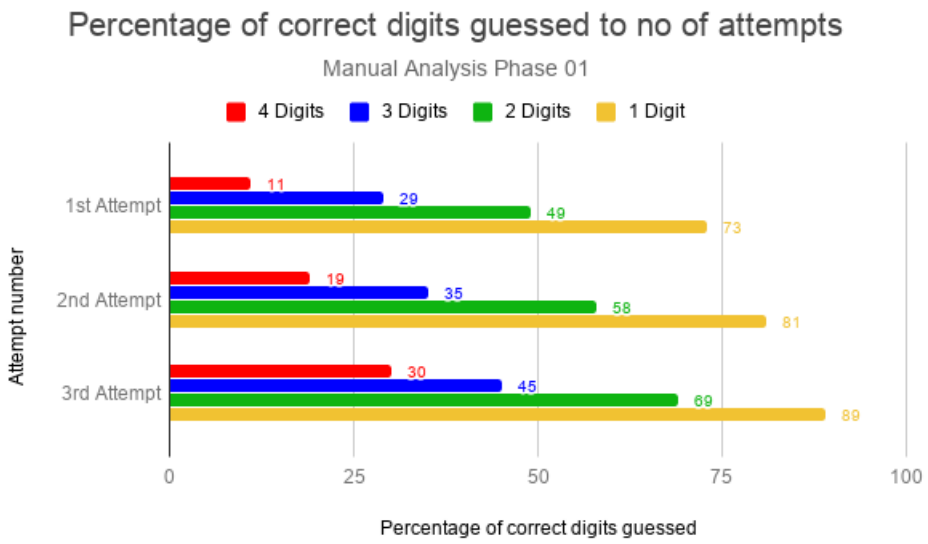

Figure 5.5: Percentage of correct digits guessed to no of attempts

As shown in Figure 5.5, the results of the Manual Analysis Phase 01 shows that 11% of accuracy has been obtained in guessing the all four digits of the PIN by all ten subjects within the first attempt while the accuracy has been increased to 19% and 30% within the second attempt and third attempt respectively. However, it was also identified that the participants of this survey were able to guess at least a single digit of the PIN with an accuracy of 73% present in a single attempt. This accuracy increases to 89% if three attempts are allowed. In each attempt, the accuracy of guessing four digits (PIN), three digits, two digits and one digit of the actual PIN has been improved with the increase in the number of attempts.

Manual Analysis Phase 02

1. Identification all four digits of the actual PIN (Exact PIN)

Actual PIN	Guessed PIN		
	1st Attempt	2nd Attempt	3rd Attempt
1789	3	8	11
2650	0	1	1
5492	1	3	5
6831	1	1	1
7153	0	7	8
9416	0	1	2
5476	4	5	7
1920	1	2	4
0163	2	3	4
3592	0	1	2

Figure 5.6: All four digits of the actual PIN – Manual Analysis Phase 02

2. Identification three digits of the correct PIN

Actual PIN	Guessed PIN		
	1st Attempt	2nd Attempt	3rd Attempt
1789	9	13	17
2650	1	1	1
5492	10	10	12
6831	2	4	5
7153	6	13	14
9416	1	6	6
5476	8	12	13
1920	6	69	11
0163	6	8	12
3592	3	6	7

Figure 5.7: Three digits of the actual PIN – Manual Analysis Phase 02

3. Identification two digits of the correct PIN

Actual PIN	Guessed PIN		
	1st Attempt	2nd Attempt	3rd Attempt
1789	15	17	17
2650	7	8	10
5492	12	12	14
6831	6	10	12
7153	10	16	16
9416	11	17	20
5476	10	12	13
1920	14	16	17
0163	11	16	19
3592	6	13	14

Figure 5.8: Two digits of the actual PIN – Manual Analysis Phase 02

4. Identification one digits of the correct PIN

Actual PIN	Guessed PIN		
	1st Attempt	2nd Attempt	3rd Attempt
1789	17	19	20
2650	11	14	17
5492	16	18	20
6831	12	16	18
7153	15	18	19
9416	15	20	20
5476	16	18	19
1920	17	19	20
0163	18	19	19
3592	13	16	16

Figure 5.9: one digits of the actual PIN – Manual Analysis Phase 02

The accuracy of the actual PIN identification in Manual Analysis Phase 02 was determined to be lower than that of Manual Analysis Phase 02 accuracy. This is due to the fact that the sample surveillance videos used for Phase 02 were captured using the prototype PIN pad as per the dimensions of the standard Large ATM PIN pad. The space between each key in this PIN pad is lower (0.635 cm horizontal

and vertical space) than the PIN pad which was designed in arbitrary dimensions used in Phase 01. Therefore, the change in the position of the forearm when the transformation between two keypresses is low when analysing the videos of Phase 02.

It showed that the accuracy of guessing the exact PIN in the first attempt by all twenty participants in the Manual Analysis Phase 02 is 6% and has increased to 16%, 22.5% with second attempts and third attempt. Identification of at least three digits, two digits and one digit of the PIN has increased with the number of attempts given to the participant.

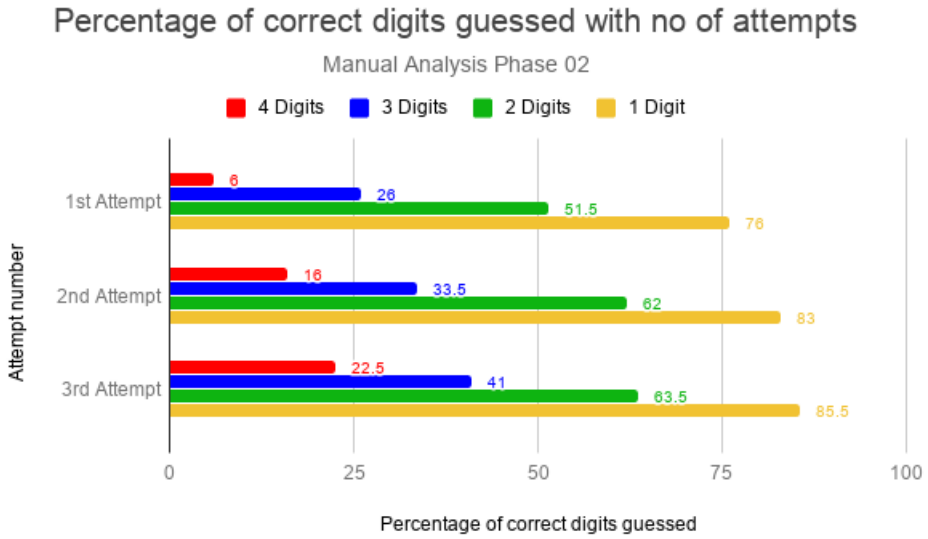

Figure 5.10: Percentage of correct digits guessed with no of attempts

5.1.2 Evaluating the Manual Analysis results against the trajectory of actual PIN to identify similar trajectory patterns

Despite the fact that actual PIN identification, when analysing the responses, it was identified that the participants of the survey have been guessed PINs which have similar trajectory movement to the actual PIN of the related sample video. Accordingly, for each PIN guessed by the participants in the survey for all the three attempts, the corresponding trajectory was plotted to identify PIN patterns.

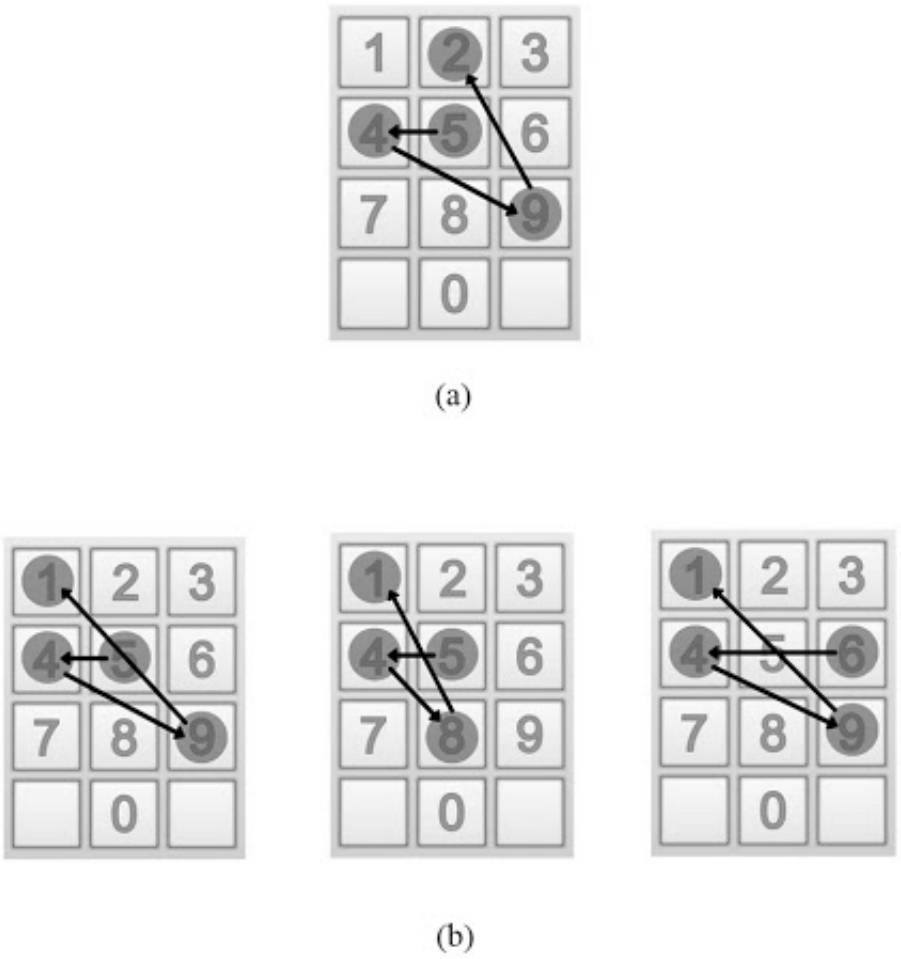

Figure 5.11: a) Actual PIN 5492 [Ground truth]. (b) PIN guessed by three subjects$_5$491, 5481*and*6491*respectively*.

Following conditions were examined when considering a PIN trajectory as similar to its corresponding correct PIN.

- When considering the trajectory of the actual PIN to the guessed PIN, the angle of the movement from one digit to another digit was exactly reviewed.
- For example; when considering the actual PIN like 5792, the shift from digit 9 to digit 2 has a left-angled movement with the digit 9. Therefore, when considering a guessed PIN as similar to the actual PIN, it was identified only the left-angled movement from the digit 9. Hence, a guessed PIN like 5731 was regarded as a similar trajectory and a guessed PIN was like 5793 as dissimilar as it has a straight angle movement from 9 to 3.

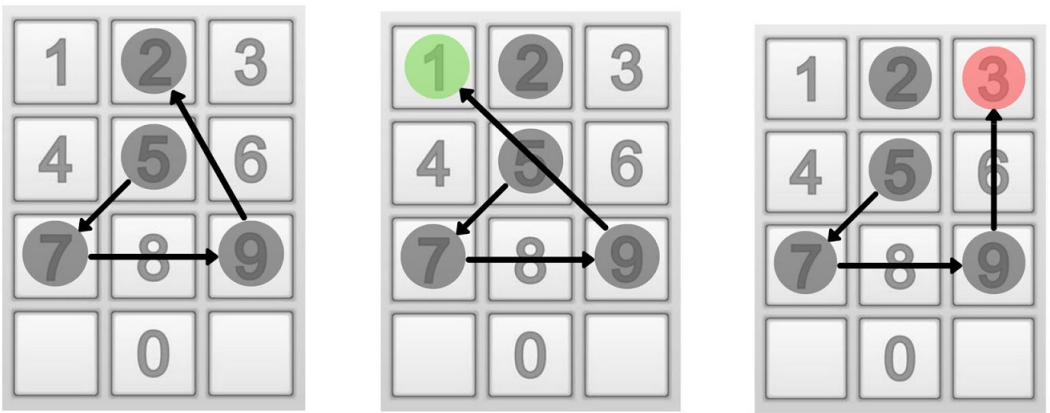

Figure 5.12: Conditions to trajectory of PIN

Manual Analysis Phase 01

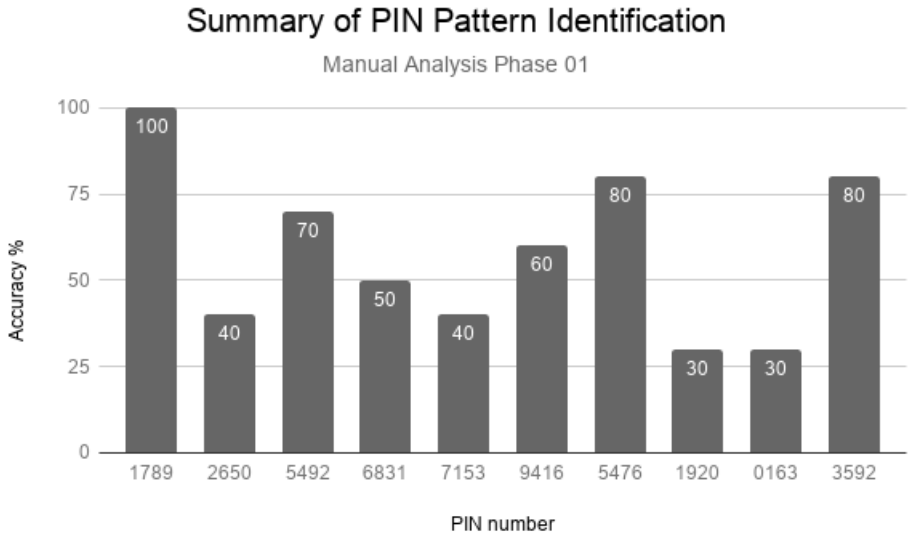

Figure 5.13: Summary of similar PIN trajectory identification - Manual Analysis Phase 01

Manual Analysis Phase 02

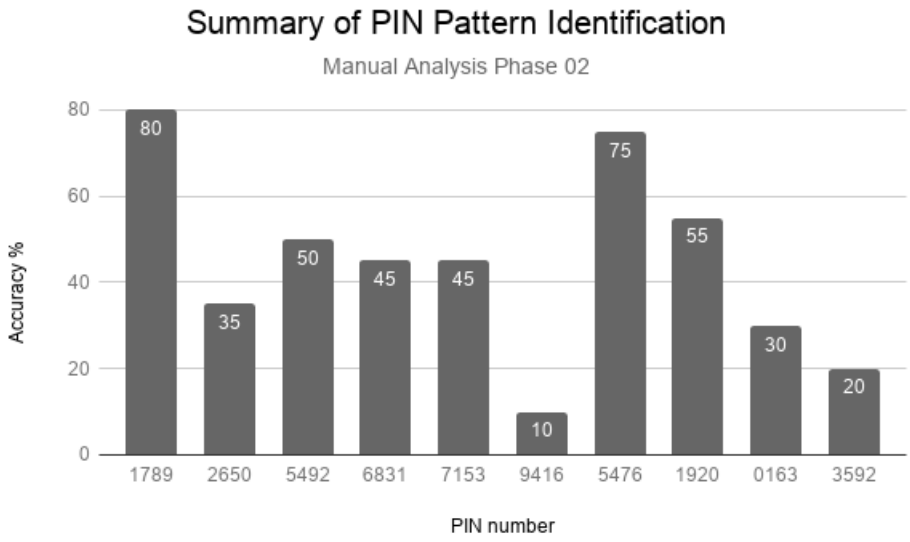

Figure 5.14: Summary of similar PIN trajectory identification - Manual Analysis Phase 02

5.2 Automated Analysis

As per the automated analysis, process to infer the PIN from surveillance footage, discussed previously, the following are the results obtained for the test data set of Subject B, making use of the x and y threshold values calculated using the data set of Subject A.

Threshold for column - 7
Threshold for rows - 11

Actual PIN	Calculated changes of columns, between presses	Calculated changes of rows, between presses	Derived PIN Possibilities
2961	[1, 0, -2]	[2, -1, -1]	2961
3651	[0, -2, -1]	[1, 0, -2]	-
9675	[0, -2, 1]	[-1, 1, -1]	6342,9675
3592	[0, 0, -1]	[2, 0, -2]	2881,3992,5004
2730	[-2, 0, -2]	[2, -2, 3]	-
6937	[2, -2, 3]	[1, -2, 2]	6937
2598	[0, 1, -1]	[1, 1, 0]	1487,2598
7401	[0, 1, -1]	[-1, 2, -3]	7401
8946	[1, -2, 0]	[0, -1, 0]	5611,8944
4903	[1, -2, 2]	[0, 1, -3]	-
9075	[-1, -2, 2]	[1, -1, -1]	-
2167	[-1, 2, -2]	[0, 2, 1]	-
1486	[-1, 1, 1]	[1, 1, -1]	2486,5709
7602	[1, -1, 0]	[0, 2, -3]	5602
0176	[0, 0, 0]	[-1, -1, 0]	7411,8522,9633,0855
0971	[1, -2, 0]	[-1, 0, -2]	0971
6015	[-1, -1, 1]	[2, -3, 2]	6018
3724	[-2, 1, -1]	[2, -2, 1]	3724
5986	[1, -1, 2]	[1, 0, -1]	1543,4876
7423	[0, 1, 1]	[-1, -1, 0]	7423

Figure 5.15: Inferred PINs for when column threshold is 7

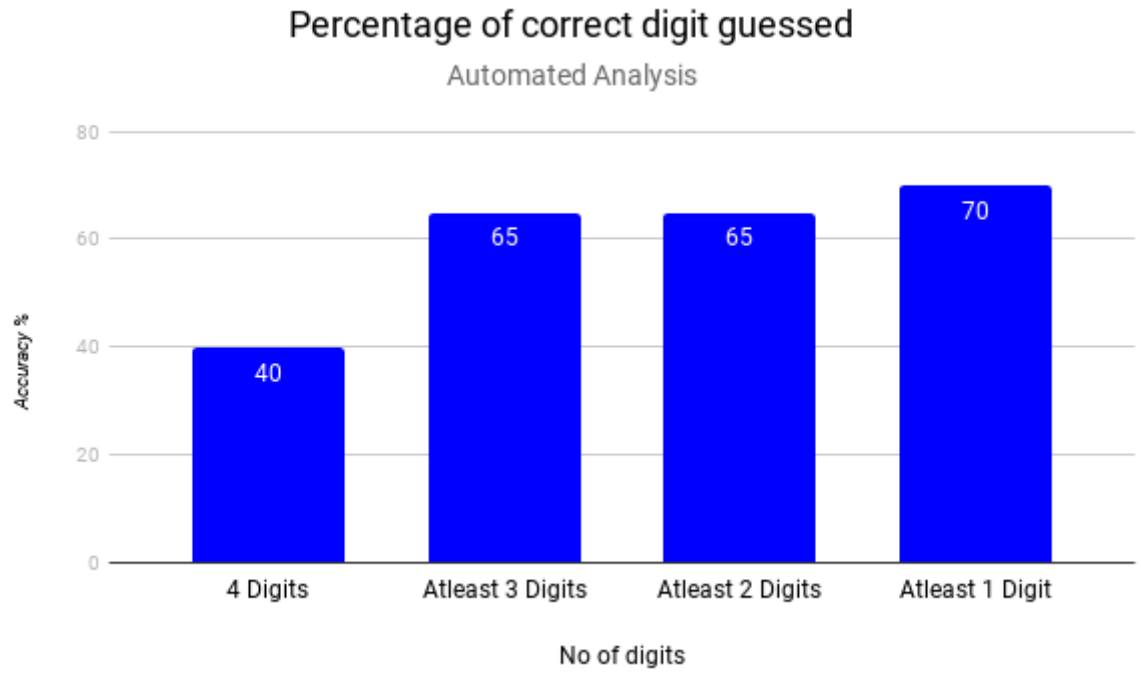

Figure 5.16: Percentage of correct digit guessed for threshold 7 - Automated Analysis

Threshold for column - 8

Threshold for rows - 11

Actual PIN	Calculated changes of columns, between presses	Calculated changes of rows, between presses	Derived PIN Possibilities
2961	[1, 0, -2]	[2, -1, -1]	2961
3651	[0, -2, -1]	[1, 0, -2]	-
9675	[0, -2, 1]	[-1, 1, -1]	6342,9675
3592	[0, 0, -1]	[2, 0, -2]	2881,3992,5004
2730	[-2, 0, -2]	[2, -2, 3]	-
6937	[2, -2, 3]	[1, -2, 2]	6937
2598	[0, 1, -1]	[1, 1, 0]	1487,2598
7401	[0, 1, -1]	[-1, 2, -3]	7401
8946	[1, -2, 0]	[0, -1, 0]	5611,8944
4903	[1, -2, 2]	[0, 1, -3]	-
9075	[-1, -2, 2]	[1, -1, -1]	-
2167	[-1, 2, -2]	[0, 2, 1]	-
1486	[-1, 1, 1]	[1, 1, -1]	2486,5709
7602	[1, -1, 0]	[0, 2, -3]	5602
0176	[0, 0, 0]	[-1, -1, 0]	7411,8522,9633,0855
0971	[1, -2, 0]	[-1, 0, -2]	0971
6015	[-1, -1, 1]	[2, -3, 2]	6018
3724	[-2, 1, -1]	[2, -2, 1]	3724
5986	[1, -1, 2]	[1, 0, -1]	1543,4876
7423	[0, 1, 1]	[-1, -1, 0]	7423

Figure 5.17: Inferred PINs for when column threshold is 7

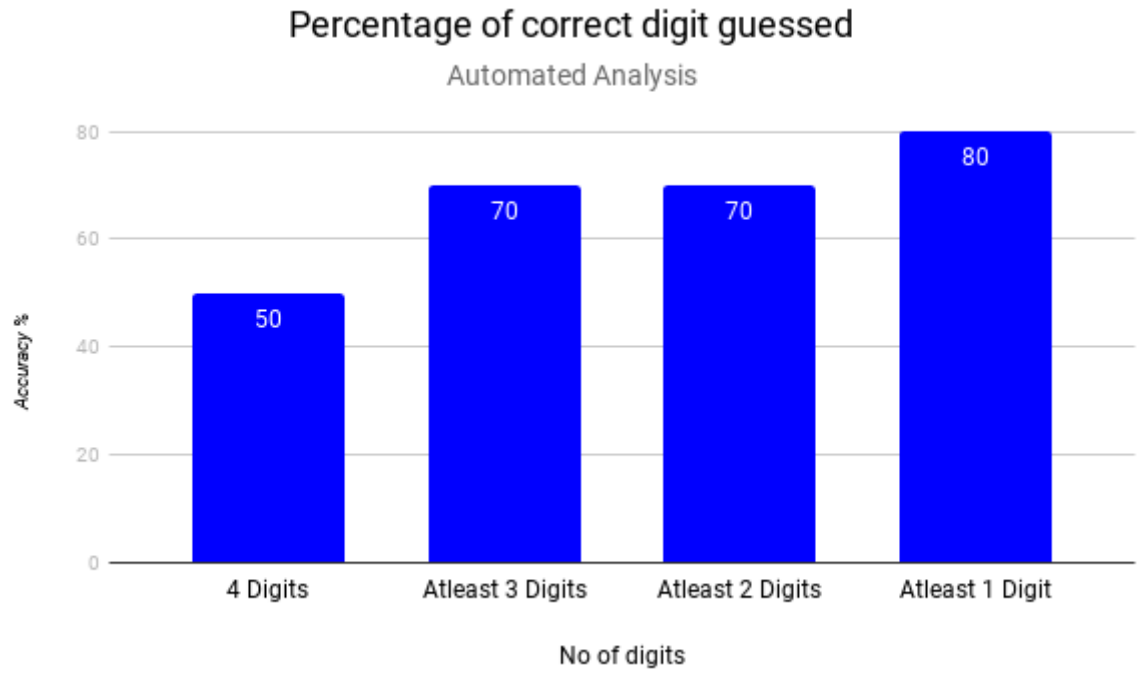

Figure 5.18: Percentage of correct digit guessed for threshold 8 - Automated analysis

Previously inferred column threshold values from the dataset of contain subject A contain 7 and 8. With the column threshold - 7 , it is possible to infer 8 exact match PINs out of 20 total PINs, which is a 40% accuracy. With the column threshold being - 8, it has improved to 10 correctly derived PINs out of 20 PINs which is 50% of accuracy. With more data gathered for subject A, the calculated result of threshold values could have been improved more precise. Hence the accuracy of inferring the correct PIN would have also been possibly increased.

Using a clustering approach to infer the most probable PIN when there are more than one corresponding PIN possibilities for certain coordinate changes

- Cluster Centroids for X coordinates - 551, 569, 592
- Cluster Centroids for Y coordinates - 574 , 582 , 612, 640

Actual PIN	Inferred set of PINs by the Algorithm	Total Deviation of actual coordinates from the cluster centroid coordinates	Suggested Most Probable PIN
9675	6342,	246	9675
	9675	214	
3992	2881	286	3992
	3992	214	
	5004	262	
2598	1487	168	2598
	2598	108	
8946	5613	205	8946
	8946	173	
9075	6842	268	9075
	9075	238	
1486	1486	211	4709
	4709	157	
3724	2724	160	3835
	3835	100	
	6068	130	
5986	1543	193	4876
	4876	181	

Figure 5.19: Distinigushing the most probable PIN from multiple suggestions

Out of the 8 instances where more than one corresponding PIN possibilities were available, 6 instances included exact match to the original PIN 1 instance included with three matching digits of the PIN 1 instance included with one matching digit of the PIN

Out of the 6 exact matching instances 5 instances and the instance with one matching digit were clearly distinguished as the most probable PIN from the available set of PINs. One exact match PIN (1486) and the Pin with 3 matching digits (2724) did not follow this heuristic. It is visible that there's a possibility to differentiate the most probable PIN when there are more than one derived PIN for a single column/row change pattern, available. However with more data points of keypress coordinates to calculate the cluster centroids for keypad columns and rows, the results could have been improved.

Chapter 6

Discussion

In this chapter, the key findings of the research and the implications are discussed with regarding the impact of video surveillance systems on ATM PIN security. Moreover, with completion of the research, the conclusions for the two research questions and the research problems formed. This chapter presents the recommendation to mitigate the risks originating with the implementation of surveillance cameras. In the future work section researcher propose further enhancements and desirable approaches to facilitate studies on this domain.

6.1 Discussion

The major finding of this research is the identification of potential threat to the ATM PIN security due to the ad-hoc implementation of surveillance cameras. During the background study it was identified that PIN entering and the keypad is clearly visible to the existing surveillance cameras inside ATM cubicles. This research also shows that the PIN can be inferred by tracking the forearm movement of the person entering the PIN even in the situations where there is no direct line of sight toward the PIN pad and the fingertips.

The threat model of the existing ATM system as discussed in section 2.5.2 does not consider the implications of possessing surveillance cameras at ATM cubicles and the potential threat for ATM PIN security. Even though surveillance cameras are installed as a physical control mechanism at ATM cubicles, it is important to rigorously consider these consequences and to have a holistic approach when developing the threat model. Therefore, it is needed to consider surveillance cameras when defining the threat boundary of the ATM system threat model. Figure 6.1 presents the threat model which was developed by the researcher considering the above aspects.

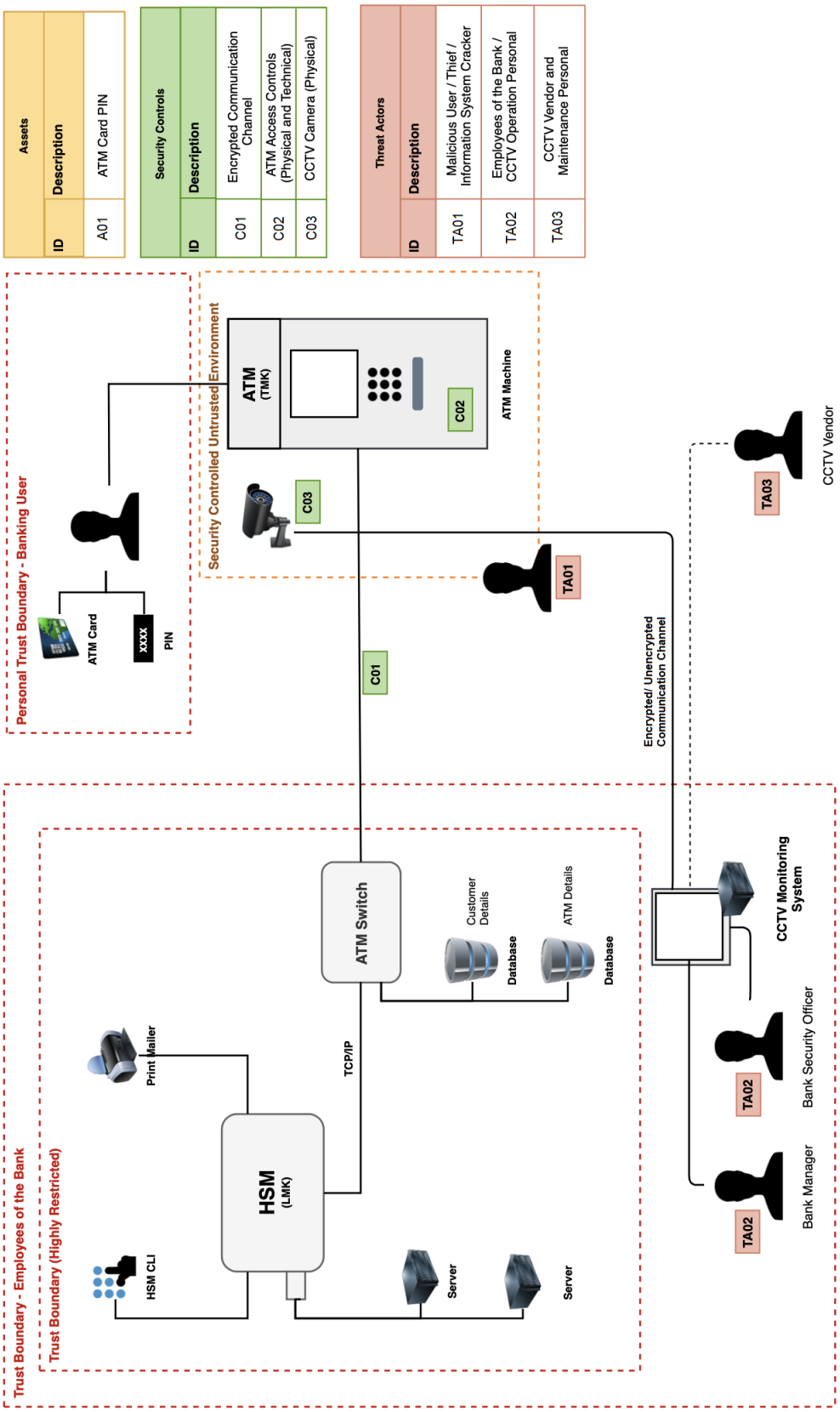

Figure 6.1: Threat model for the existing ATM system

As presented in Figure xx, the communication channel between the surveillance

camera systems (CCTV camera) and the CCTV monitoring system where the camera footage is stored are either encrypted or unencrypted. The surveillance camera system which is in the untrusted boundary is communicating via an encrypted or unencrypted channel to the trust boundary of the ATM system. PIN data are stored in HSM which is in a highly restricted trust boundary. Yet, the unencrypted storage of surveillance cameras which has the potential of revealing the ATM PIN comes out the this restricted trust boundary. Therefore, the security of the ATM system should provide appropriate controls addressing these implications. Consideration of this holistic approach when developing the ATM system assists the whole banking system to comply with basic principle of confidentiality.

The significant contribution of this research is the identification of exact PIN with 50% accuracy, even in the situations where keypad and the movement of the fingertip are not visible to the attacker. Aside from methods proposed in the existing literature[cite], a novel computer vision based method was introduced for the identification of the keypress events. In this method, it is showed that detection and tracking of the forearm movement and calculation of the gradient was sufficient to identify the keypress events. The PIN guessing algorithm is another noteworthy contribution of this research. Moreover, for given x,y coordinates of keypress events, the PIN can be identified using the algorithm discussed in section 4.XXX, where the threshold for column/row separation can be collected. Furthermore, thresholds for row/column movements were obtained from one user while PINs were guessed for a different user. In fact, it was proved that even an attacker can obtain the threshold values from intentionally inserting different PIN combinations to calculate the thresholds and use it on any other user. Therefore, the automated PIN guessing process developed during the course of research exhibits the possibility of generalization. Hence maximizes the threat by providing the capability to obtain large no of PIN for different users and also several attempts for a single user.

This research only used a dataset of 20 sample videos yet record a 50% of accuracy which affirms this approach can be used with small dataset other than the machine learning approaches which require large number of data.

However, it is confirmed that bounding box based object tracking and detection using OpenCV tracking API which has been employed in previous studies[cite] is not suitable to track the slight movement of the forearm during the PIN entering process.

6.2 Conclusion about the research question

What is the potential to discover the ATM PIN through visual surveillance of CCTV video footage?

It was identified that in some situations PIN is clearly visible and there is high potential to identify the PIN due to current practice of installing surveillance cameras. The experimental setup was created for conditions where the PIN pad and fingertips are not visible to the attacker unlike the previous studies to create an unfavourable situation for an attacker. Still the results of the manual analysis indicate that it is a 22.5% potential to identify the exact PIN and the trajectory of the PIN pattern with observing the naked eye. Automation of the PIN guessing process maximizes the potential to 50% which upholds that there is considerable potential of a threat to ATM PIN security.

What are the threats of revealing the ATM PIN and what is the impact on the banking system?

During the course of the research, it was identified that the basic trust assumption of confidentiality in the ATM system is violated due to the ad hoc installation of surveillance cameras at ATM cubicle. The existing threat model of the ATM system does not consider the surveillance camera system. It results in negative consequences for the ATM PIN security. Therefore, a holistic approach of the threat model for the ATM system considering the aforementioned aspect is presented in this research.

6.3 Conclusion about the research problem

The findings of the research substantiate that the installation of surveillance cameras originate a threat to security-sensitive information. Accordingly, there are negative consequences of the use of surveillance cameras as a physical security control. Inference of the PIN using video footage present the possibility of vision-based attacks utilizing surveillance cameras. Background study and the results of the manual and automated PIN guessing processes confirm that existing installation of surveillance cameras inside ATM cubicles violates the PIN security. Thus the surveillance cameras should be considered when developing the threat model of an information system.

6.4 Recommendation

As per the results and the discussion of the research, the recommendations suggested by the researchers are mentioned as follows.

The basic assumption is that the ATM PIN is not known by any party (in/out of bank) other than the user. As previously discussed a threat model has been created focusing on the asset PIN and according to that threat model, the operational security of the ATM system has been implemented to avoid violating the aforementioned assumption. The ATM PIN is perfectly secured well within that operational environment. The main discovery of this research is that the boundary of security of the ATM PIN, ends with accomplishing the operational security aspect and no further investigation hasn't been done on other aspects. Through this research it is visible that there is a possibility of using the surveillance camera inside of the ATM cubicle (which is a physical security control implemented by the bank itself), to infer the user's typed PIN. Hence the researchers strongly highlight and suggest to pay more attention when defining the boundary of the threat model for ATM PIN, not limiting to its operational security only, but also include these kinds of security implications from not often considered, other factors as well.

This research reveals the lack of existing guidelines and best practices and the actual practice of such guidelines, related with the surveillance cameras, causes a considerable threat to security sensitive information such as ATM PINs. The researchers suggest introducing new rules, regulations, guidelines and best practices and updating existing standards for installation of surveillance cameras in environments with such security sensitive information, by the authoritative bodies. And also when installing surveillance cameras, the security implications of those surveillance cameras on sensitive information, should be addressed with more concern.

Even if the current ad hoc surveillance camera placement does not pose a considerable threat of revealing the PIN, banks should consider relocating or adjusting the already installed CCTV surveillance system when there is an upgrade and/or relocation of ATM machine(s). Furthermore, these findings can be used to reengineer the ad hoc CCTV camera installation process at ATM cubicles.

We also recommend to securely store the video footage from the CCTV cameras inside the ATM cubicles. Such recordings should be accessed on in the case of a complaint or a dispute. Even in such a situation, the video should be viewed by an authorized official of the bank.

Another recommendation of this research is to sanitize the video footage so that the PIN entering process could not be identified. One probable way of doing this is to obscure the area of the footage where the PIN entering process happens (ex - keyboard are, subject's arm). Another way is to reduce the frame rate of the video footage. The methodology which is used in this research heavily relies on being able to identify the keypress and the coordinates of those keypresses from the movement of the subject's arm. With reduced frame rate it would be difficult

to apply such an attack scenario since the available frames of the footage might not contain enough data to analyse and infer the typed PIN. And also using the cubicle surveillance just for the intended purpose by capturing the frames which identifies the subject who enters the ATM and capturing the frames of the cash dispensing slot (if that's a requirement of the bank) without compromising the keypad and discarding other set frames from the video would limit the use of such attack scenario on ATM PIN.

And also, it is important to educate the banking staff as well as the customers about the potential aspects of threats to PIN security, so that they would be knowledgeable enough to avoid them.

6.5 Future Work

This research shows that the currently defined boundary for ATM PIN security ends with achieving operational security of the ATM system, but the presence of a CCTV camera inside the ATM cubicle which is implemented by the bank itself poses a threat of revealing the user's ATM PIN. This raises the question of where the line should be drawn when designing a threat model for PIN security. The surveillance camera system is itself a part of the banking system but not considered when building the threat model for the ATM PIN. As recommended by the researchers, it is vital to take such factors also into consideration as well, which leads to another question. How far those other factors should be considered. For example, there can be situations, where there can be other surveillance cameras implemented, in the near vicinity of the ATM machines. (ex: open ATM machines at malls) and even the mere location of the ATM could be a factor that would lead to compromisation of the ATM PIN in situations like where any person has a clear vision towards the ATM keypad itself for example ATMs in low grounds and the observer in a high ground. Researchers suggest more study on boundary selection in threat modelling for ATM PIN security to be carried out.

In this research, only a proof of concept was built to demonstrate the potential threat scenario. Therefore, researchers have employed simple marker-based tracking. However, this approach can be extended using advanced algorithms and technologies specifically developed for hand/body part tracking. The algorithm used to filter out the most probable PIN in situations where the row/column changes for a PIN corresponds to more than one PIN is just an attempt to heuristically see the possibility of such an approach, in this research which is proven to be effective with the dataset gathered. The calculated cluster centroids for the columns and rows depend on the coordinate dataset itself. The concern is that depending on the tracked point of the subjects forearm, the set of inferred

coordinates of keypresses for each subject could be different. This research only incorporates two subjects (Subject A and B) to gather video data of typed PINs; Subject A's dataset is used to calculate the threshold values to identify the changes of column/rows of the keypad between keypresses and those calculated threshold values are used in the algorithm to output the probable PINs from Subject B's dataset. Involving more subjects to gather video data is encouraged since it would provide a more robust dataset. And also more volume of a video dataset would enable the use of a machine learning approach to infer and analyse the typed PIN from the video dataset. Based on the finding of this research, this work can be extended as an audit tool. Which can be used to evaluate the potential threat caused by the installation of a surveillance camera. The following figure depicts high-level architecture to such a tool.

References

[1] *Standard: PCI PIN Transaction Security Point of Interaction Security Requirements (PCI PTS POI) Information Supplement: ATM Security Guidelines*. 2013.

[2] C. B. of Sri Lanka.

[3] 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.

[4] Y. Xu, J. Heinly, A. M. White, F. Monrose, and J.-M. Frahm, "Seeing double: Reconstructing obscured typed input from repeated compromising reflections," in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, pp. 1063–1074, ACM, 2013.

[5] R. Raguram, A. M. White, D. Goswami, F. Monrose, and J.-M. Frahm, "ispy: automatic reconstruction of typed input from compromising reflections," in *Proceedings of the 18th ACM conference on Computer and communications security*, pp. 527–536, ACM, 2011.

[6] D. Shukla, R. Kumar, A. Serwadda, and V. V. Phoha, "Beware, your hands reveal your secrets!," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pp. 904–917, ACM, 2014.

[7] C. B. of Sri Lanka, "Annual report 2018 — central bank of sri lanka, financial sector performance and system stability," 2018.

[8] "Payments and settlements department central bank of sri lanka."

[9] C. B. of Sri Lanka, "Financial instruments deposits,"

[10] C. B. of Sri Lanka, "Objectives, functions & organization," jun 2014.

[11] C. B. of Sri Lanka, "Payment and settlement systems act, no. 28 of 2005," sep 2005.

[12] C. B. of Sri Lanka, "Payment and settlement system circular no 01 of 2019," feb 2019.

[13] "Directions, determinations, and circulars issued to licensed commercial banks (inclusive of amendments made up to 30 november 2013)."

[14] C. B. of Sri Lanka, "Baseline security standard for information security management, assurance level 1, version 1.0,," nov 2013.

[15] N. Shevchenko, T. A. Chick, P. O'riordan, T. P. Scanlon, and C. Woody, "Threat modeling: a summary of available methods," *no. July*, 2018.

[16] C. B. of Sri Lanka, "Credit card operational guidelines," jan 2010.

[17] A. Costin, "Security of cctv and video surveillance systems: Threats, vulnerabilities, attacks, and mitigations," in *Proceedings of the 6th international workshop on trustworthy embedded devices*, pp. 45–54, ACM, 2016.

[18] L. Wu, X. Du, and X. Fu, "Security threats to mobile multimedia applications: Camera-based attacks on mobile phones," *IEEE Communications Magazine*, vol. 52, no. 3, pp. 80–87, 2014.

[19] B. Cusack and Z. Tian, "Evaluating ip surveillance camera vulnerabilities," 2017.

[20] M. Coole, A. Woodward, and C. Valli, "Understanding the vulnerabilities in wi-fi and the impact on its use in cctv systems," 2012.

[21] K. Mowery, S. Meiklejohn, and S. Savage, "Heat of the moment: Characterizing the efficacy of thermal camera-based attacks," in *Proceedings of the 5th USENIX conference on Offensive technologies*, pp. 6–6, USENIX Association, 2011.

[22] D. Balzarotti, M. Cova, and G. Vigna, "Clearshot: Eavesdropping on keyboard input from video," in *2008 IEEE Symposium on Security and Privacy (sp 2008)*, pp. 170–183, IEEE, 2008.

[23] F. Maggi, A. Volpatto, S. Gasparini, G. Boracchi, and S. Zanero, "A fast eavesdropping attack against touchscreens," in *2011 7th International Conference on Information Assurance and Security (IAS)*, pp. 320–325, IEEE, 2011.

[24] K. Jin, S. Fang, C. Peng, Z. Teng, X. Mao, L. Zhang, and X. Li, "Vivisnoop: Someone is snooping your typing without seeing it!," in *2017 IEEE Conference on Communications and Network Security (CNS)*, pp. 1–9, IEEE, 2017.

[25] A. T.-Y. Chen, M. Biglari-Abhari, I. Kevin, and K. Wang, "Context is king: Privacy perceptions of camera-based surveillance," in *2018 15th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS)*, pp. 1–6, IEEE, 2018.

Appendices

Appendix A

Backgound

A.1 Questionnaire for Interviews

Identification of side-channel vulnerabilities in surveillance camera footage: Inferring security-sensitive keyboard inputs

Researchers:
Dilanka Perera: dilankaperera95@gmail.com
Harinda Samarasekara: samarasekara.harinda@gmail.com
Piyumi Seneviratne: piyumisenevirathne@gmail.com
Supervisor: Dr C.I.Keppetiyagama | cik@ucsc.cmb.ac.lk

Following are the questions to be investigated during the discussion for the above-mentioned research.

1. Are there a particular vendor(s) to install ATMs?
    a. Are they work on constructing the kiosk as well for the ATM?
    b. Do they install Surveillance camera system (SCS) for the ATM kiosk?
        i. If NO, is there a separate vendor or multiple vendors?
2. What is the process of installing ATM kiosks?
    a. Does it require permission from CBSL?
    b. Is a Feasibility study need?
    c. Do any documents need to submit to CBSL?
3. Do the SCS providers/vendors have predefined guidelines to install CCTV in ATM kiosks?
    a. If YES,
        i. What are they?
            1. How many cameras?
            2. What is the quality of those cameras? (Do they change or have a specific standard?
            3. Any specific position? Eg: focus on the door/ not seeing the keypad
        ii. What are the ways or how to inspect the level of security it preserved?
    b. If NO;
        i. Who create guidelines/policies for the installation process of SCS?
        ii. what are they?
            1. How many cameras?
            2. Any specific position? Eg: focus on the door/ not seeing the keypad
        iii. What are the ways or how to inspect the level of security it preserved?
4. Are any guidelines provided by CBSL regarding the installation of SCS in ATM kiosk?
    a. If YES,
        i. What are they?
        ii. What are the ways or how to inspect the level of security it preserved?
        iii. Does any party from CBSL visit and verify the security level of SCS?
            1. If Yes, How?
        iv. Are there any documents to submit to CBSL?
5. In the bank, who has access to surveillance camera footage? (Centrally handle or branch wise)
6. Is there any monitoring or fraud detection process currently available using surveillance camera footage?
    a. If YES, how?
7. Are there any frauds reported at ATM kiosk regarding stealing of user information (PIN)? Eg: Card skimming
    a. Using surveillance camera footage?

Figure A.1: Summary of Bank Interviews

Appendix B

Methodology

B.1 Manual Analysis Survey

Identification of side-channel vulnerabilities in surveillance camera footage: Inferring security-sensitive keyboard inputs

University of Colombo School of Computing

Dilanka Perera: dilankaperera95@gmail.com
Harinda Samarasekara: samarasekara.harinda@gmail.com
Piyumi Seneviratne: piyumisenevirathne@gmail.com

As a part of our research for the Degree of Bachelor of Science Honours in Information Systems, we are conducting a survey *to investigate the probability of manually inferring the PIN(Personal Identification Number) through surveillance camera footage of PIN entering process.*

We will appreciate if you could complete the following survey.

Any information gathered in connection with this study that can be identified with you will remain confidential.

Respondent Details

Name:

Email:

Year of study:

Instructions

We will provide you with twenty(10) video footage of twenty(10) different PIN entering processes of an ATM scenario. Each PIN has 4 unique digits. Observe how the hand of the user who is entering the PIN is moving across the ATM keypad in each video. Guess and identify the PIN which is entered in the video and mention it in the corresponding table as provided below. We will provide you with 3 attempts to observe the video and guess the PIN at each attempt.

Following is a prototype of the ATM keypad for your reference.

Figure B.1: Manual Analysis Survey

B.2 Manual Analysis Survey

Sample Video Number	Guessed PIN		
	1st Attempt	2nd Attempt	3rd Attempt
01			
02			
03			
04			
05			
06			
07			
08			
09			
10			

2

Figure B.2: Manual Analysis Survey

B.3 Marker Based Hand Detection and Tracking

boundbox_tracker.py

```
58          (success,box)=tracker.update(frame)
59          # print ("frameNo = " +str(frame_no))
60          # print (type(box))
61
62
63
64          if success:
65              # draw bounding box
66              (x,y,w,h)=[int(v)for v in box]
67              cv2.rectangle(frame,(x,y),(x+w,y+h),(0,255,0),2)
68              # get centroid of the box
69              # cx,cy=get_cx_cy(box)
70
71          #updte frame counter
72          # fps.update()
73          # fps.stop()
74
75          # information to display
76          info=[
77              ("Tracker",tracker),
78              ("Success","Yes"if success else "No"),
79              # ("FPS","{:.2f}".format(fps.fps())),
80              ("Frame No",frame_no),
81          ]
82          for (i,(k,v))in enumerate(info):
83              text="{}:{}".format(k,v)
84              cv2.putText(frame,text,(800,(i*20)+350),cv2.FONT_HERSHEY_SIMPLEX,0.6,(255,0,0),2)
85              # append cx,cy and frame no to pandas Dataframe.
86
```

Figure B.3: Tracking with Bounding Box

B.4 Marker Based Hand Detection and Tracking

colour_thresholding.py

colour_thresholding.py > fig

```
90
91
92          # apply mask to find marker
93          hsv=cv2.cvtColor(frame,cv2.COLOR_BGR2HSV)
94          mask = cv2.inRange(hsv, lower_range, upper_range)
95          cv2.namedWindow('output1',cv2.WINDOW_NORMAL)
96          cv2.resizeWindow('output1',600,600)
97          cv2.imshow('output1',mask)
98
99          # find contours of the marker
100         contours =cv2.findContours(mask,cv2.RETR_TREE,cv2.CHAIN_APPROX_SIMPLE)
101         # print(contours)
102         cnts=imutils.grab_contours(contours)
103         center=None
104
105         if len(cnts)>0:
106             # print(type(cnts))
107             # print(len(cnts))
108             # print(cnts)
109             c=max(cnts,key=cv2.contourArea)
110             ((x,y),radius)=cv2.minEnclosingCircle(c)
111             # print("radius")
112             # print(radius)
113             # print(x,y)
114             M=cv2.moments(c)
115             # print(M)
116             if M['m00'] > 0:
117                 center= (int(M["m10"] / M["m00"]), int(M["m01"] / M["m00"]))
```

Figure B.4: Colour Thresholding

Appendix C

Results

C.1 Manual Analysis Phase 01 Results

Correct PIN	Guessed PIN	Attempts	Name of the participant									
1789		1st	3245	3456	1789	2456	1478	1789	1789	1759	1789	1789
		2nd	1478	1456	1789	1456	1456	1789	4789	1756	1789	1789
		3rd	1789	1456	1789	1456	1789	1789	1489	1789	1789	1789
2650		1st	1547	3586	4578	2467	1578	1567	2638	1247	6457	1350
		2nd	1578	1470	1478	2647	1345	1890	1679	1347	1457	2350
		3rd	1570	1470	1457	2647	1647	1890	1578	1357	1570	2650
5492		1st	1342	7532	5471	2152	5491	6491	7082	3182	1590	5491
		2nd	1423	1452	5481	2152	5491	5491	2489	2193	5481	5491
		3rd	5492	1482	5481	5485	5491	5491	2189	5491	5491	5492
6831		1st	1451	7451	6541	5721	2421	4731	1782	2731	9731	5731
		2nd	3521	4521	6521	5721	5754	5731	2426	2731	9731	5731
		3rd	1732	4521	5421	5721	5754	5721	2752	2731	9731	5721
7153		1st	4253	7521	4731	1753	7593	7153	1452	4253	8052	7152
		2nd	7182	7452	4721	7153	7153	7153	4152	5789	0452	7153
		3rd	7453	7452	7152	7453	7152	7153	7485	2483	_0952	7153
9416		1st	8415	0754	8415	5412	9413	8719	8438	8453	9715	9426
		2nd	8412	0758	8415	8715	9416	8719	8745	1539	9715	9416
		3rd	8715	0758	8415	9715	8416	8719	8415	8415	9715	9416
5476		1st	5470	5478	5476	5473	5476	8703	5785	5476	5478	5473
		2nd	2175	5478	5476	5476	5476	8703	5785	2175	5475	5473
		3rd	5476	5476	5476	6473	5476	5473	5486	2173	6575	5476
1920		1st	1527	1750	1547	4903	4917	1950	5784	1924	5170	1920
		2nd	1847	1048	1547	8903	1927	1920	8480	1750	4810	1920
		3rd	1057	1048	1547	8920	1918	4920	8780	4810	4810	1920
0163		1st	8142	1041	7152	0463	7163	8461	7152	0153	0153	0193
		2nd	7152	1052	7153	0463	7152	0461	0728	0193	0182	0193
		3rd	7452	0452	7153	0563	7452	0761	0758	0163	0152	0163
3592		1st	2481	1407	3781	3592	2481	3491	2485	2451	-	2481
		2nd	2405	1407	3481	2481	3592	3491	3486	2481	5849	2481
		3rd	2401	2408	3451	3592	2481	6791	2458	2481	2481	2481

Figure C.1: Manual Analysis Phase 01 Results

C.2 Manual Analysis Phase 02 Results

	Guessed PIN	Attempts	Name of the participant									
			1. Kavinda	2. Oshan	3. Manisha	4. Janani	5. Ananda	6. Hiruni	7. Salitha	8. Eranda	9. Logeesan	10. Dilran
		1st	1796	-	1486	-	1789	1409	1489	7809	4789	1789
		2nd	1789	1789	1456	2089	1789	1709	1789	7809	4789	4789
1789		3rd	1789	1789	-	1789	1789	1789	1789	7809	4789	1789
		1st	2358	-	2--0	-	-	1247	1235	4870	1587	1547
		2nd	2315	1547	5980	23--	2579	1247	1547	4870	1578	1547
2650		3rd	2135	-	-	2340	2547	1457	2647	1540	1357	1548
		1st	5462	-	-	5491	5491	5462	2451	7893	1493	2162
		2nd	5462	21--	--91	5491	5461	5461	2451	8793	5793	2161
5492		3rd	5462	2193	2591	5491	5491	5492	2451	8793	5793	5491
		1st	2531	-	36--	3021	5731	2531	5712	6931	4721	3581
		2nd	2831	-	3561	3021	5731	3521	5712	6931	4721	3521
6831		3rd	2831	6732	3521	3021	5831	5721	5712	6931	4731	3521
		1st	7453	-	7-63	-	7453	7152	7453	8263	8463	7453
		2nd	7453	7153	7453	7153	7153	7152	7153	8263	8463	7453
7153		3rd	7453	-	7456	7153	7153	7152	7153	0263	8463	7453
		1st	8412	-	-	6413	8412	9413	9843	9742	9761	6415
		2nd	8413	6413	04-6	9413	8413	9716	9413	9745	9741	6415
9416		3rd	_0413	-	9746	9513	8413	9716	9416	9412	9746	6415
		1st	8543	2146	54--	-	5476	5476	5472	9806	5476	2145
		2nd	5143	-	5476	2143	5476	5476	8472	5486	5476	5473
5476		3rd	5143	-	-	2143	5476	5476	5472	5486	5476	5473
		1st	9240	-	1957	1920	4720	1928	1947	5920	7904	1928
		2nd	9240	1920	1958	1920	5920	1628	1947	5920	7980	1958
1920		3rd	9240	-	1950	2910	2630	1920	1947	5920	7904	1928
		1st	_0132	_0462	0163	0153	0462	0463	8462	0132	0763	8132
		2nd	_0132	-	0163	0153	0462	0163	8153	0162	0763	8163
0163		3rd	_0163	_0463	-	0463	0462	0162	8153	0162	0463	8162
		1st	5892	-	2-93	5803	2481	8694	6895	6892	2793	-
		2nd	5891	2461	2591	5803	2481	3592	6895	6892	2791	3561
3592		3rd	5891	-	2591	5803	2482	3592	3562	6892	2791	2591

Figure C.2: Manual Analysis Phase 02 Results

Appendix D

Code base

All the code bases used in this research can be found in the following github repositories.

- **URL** https://github.com/harinda05/handtracker
- **URL** https://github.com/harinda05/Pin-Inferring-from-Numeric-Keypad
- **URL** https://github.com/piyumiS/KeyPressDetection