Effectiveness of Atm and Bank Security: Three Factor Authentications With Systemetic Review

EFFECTIVENESS OF ATM AND BANK SECURITY: THREE FACTOR AUTHENTICATIONS WITH SYSTEMETIC REVIEW

RKAR. Kariapper[1], MS. Suhail Razeeth[2], P. Pirapuraj[3] and ACM. Nafrees[4]

[1,3,4] South Eastern University of Sri Lanka
[2] Sabragamuwa University of Sri Lanka

[*]Corresponding author e-mail: rk@seu.ac.lk

Abstract. Security is one of the key aspects in despite of time, location and domain. Providing a better security is an essential obligation to all sectors (state and private) and workers. Rendering better security is not only difficult but also fairly impossible due to growth of new technologies and constantly growing Information Technology domain. Rapid Improvement of banking sector provides many acceptable ways of managing the accounts, information and activities. This advancement has been a main driving force to the account activities with the help of Automatic Teller Machine (ATM). With the increase number of ATM usage among the public, hackers also use the technological growth to hack the data / information and apply the fraud actions. The said vulnerabilities have been increasing in a gradual manner and also ATM fraud has spread and become nightmare all around the world. This paper elaborates to mitigate the possible frauds can be happened at the ATM cubical with the hybrid multi-layered security concept. Here, previous studies were reviewed and compared in order to support to develop a system with the less loopholes. A three-layered architecture including PIN, OTP or finger print and pattern lock has been used in this system to mitigate the frauds. 400 students were selected to test the system and 384 students roughly 96% of students have successfully entered their pin number at the first attempt, in the second layer 95% of the students out of 384 students were succeeded and the third layer 99% of the students out of 363 students were success in drawing the patterns. The overall result of this evaluation process shows that, the suggested security tiers can be applicable since the accuracy in performance is better and accepted by the sample selected.

Keywords: ATM, OTP, fingerprint, pattern lock, security

1. Introduction

Security is one of the key aspects in despite of time, location and domain. Providing a better security is an essential obligation to all sectors (state and private) and workers. Rendering better security is not only difficult but also fairly impossible due to growth of new technologies and constantly growing Information Technology domain.

Rapid Improvement of banking sector provides many acceptable ways of managing the accounts, information and activities. This advancement has been a main driving force to the account activities with the help of Automatic Teller Machine (ATM). Nowadays, ATM are enormously used by public since easy access, user friendly and promptly availability of cash at any place. Hence, it is important to provide security in different form to avoid the heist of money from the ATM. Hackers use the

technological growth to hack the data / information and apply the fraud actions. The said vulnerabilities has been increasing in a gradual manner (Singh, Ayub, & Verma, 2013) and also ATM fraud has spread and become nightmare all around the world(Kumar, 2014).

Traditional ATM machine works with only one verification which is pin number, when a user enters the correct pin stored in the database, the user is able to do his /her transaction. This approach is very weak and less in security measure. Hackers easily snatch the money from bank as via using accounts hacking and card frauds, pin heist methods respectively. On the other hand, ATMs are being cheated and robbed in many areas, although it has high security protocol and procedure. It is important obligation to the person in-charge to construct a security barrier in order to evade this kind of crimes.

The Aim of this paper is to implement a three-factor authentication against ATM card heist and also compare previous relevant studies to recommend a best ATM security model for banking sectors.

2. Atm Fraud Methods

Nowadays ATM fraud is very common and the followings are some of the common and important methods.

2.1. Shoulder suffering:

It is the way toward watching, when someone entering pin number at the ATM. Keeping more than one ATM machines in a single cube leads this problem more (Lija & Santo Varghese, 2017).

2.2. Hidden camera:

Pin number has been caught by different imaging gadget, for example, camera and camera focal point. This is one of the standout amongst the most well-known techniques these days (Oškrdalová, 2016).

2.3. Skimmer:

Skimming is a strategy utilized by programmers to catch secret information from the magnetic strip of an ATM card(Hodges, 2018).

3. Sequence Diagram Of Traditional Atm Procedure

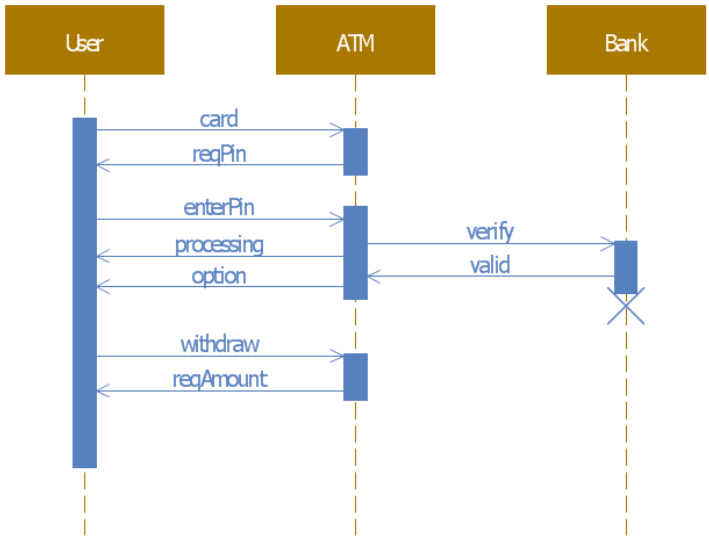


Figure 1: Sequence Diagram Of Normal ATM Transection("SEQUENCE DIAGRAM OF TRADITIONAL ATM PROCEDURE," N.D.)

4. Litrature Review

4.1. General Review

It was identified that computer generated number with biometric security has reduced the risk of being hacked rather than using only with pin security (Bhosale, 2014). *G. Renee Jebaline* and *S. Gomathi,* said that biometric authentication is a process or ability of individual to prove his or her own identity using biometric input or authenticate ourselves in case of ATM transactions (Jebaline & Gomathi, 2015). Mohsin Karovaliya et al. from their study, it can be identified that in the case of biometric technologies Iris and Retina always have its higher performance of security when compared with face and fingerprint plus cost, accuracy and stability. Meanwhile fingerprint method provides higher stability and medium accuracy with lower cost(Karovaliya, Karedia, Oza, & Kalbande, 2015).

4.2. ATM Card Heist Review

Also, Mohsin Karovaliya et al from their study they suggested a system that working with one-time password (OTP) and facial recognition features. In this system user first needs to swipe the particular card and the bank ATM camera check the face of the ATM user from the database. If the face is matched with database then a onetime password will be sent to phone. The user uses that pin and can-do ATM relevant work. In case, if the camera finds more than one user in the ATM cube, it blocks the account for security purpose. So it will be affective system for getting more accurate security level in ATMs(Karovaliya et al., 2015). And also, this OTP is working with random number generator techniques as well as MD5 hashing techniques.

Also Mohammed Hamid Khan from his study found a security system for ATM by using Biometrics and OTP. In this system, particular person must use his pin into ATM, once the person used the pin the ATM give two options either they want to select OTP or Biometric. If they select OTP then person get message from his phone and can use. If not they can be used Finger print to access further(Hamid, 2015). This is better option when compare with traditional pin system and also it provides flexibility like giving fingerprint option in case of problems arise in phone.

B.V. Prasanthi et al found a method which works with Palm Vein Biometric Technology to protect against ATM issues. In their system they also have used two-way verification system by Palm Vein Technology and user identification number (UIN). Bank gathers the UIN when user creates account into particular bank and when they want to use the ATM, they need to scan their hand with palm sensor and then it will check the palm Vein and UIN. If it is matched the transaction can be proceeded, if not it will be rejected. This method also bit technologically advance rather than commonly used pin method. At the same time, the major drawback is, only particular person can access this system, In case of emergency there is no substitution due to its uniqueness and pattern matching attributes (Prasanthi, B. V., Hussain, S. M., Kanakam, P., Chakravarthy, 2015).

Lusekelo Kibona worked with two-way verification system and suggested a method. In his security system, user initially needs to use his or her card and pin for primary step verification. Once it become success, then it moves to second step verification. If not, user must give the correct pin again. The second level verification is facial recognition. If the face image matches with user repository image in the bank then transaction will be allowed, if it is not matched then it will hold the card inside the ATM and send a message to bank staffs. The main drawback with this system is; that in case of emergency, others cannot use this system, meanwhile it protects money stealing from theft(Kibona, 2015).

Moses O. Onyesolu and Amara C. Okpala proposed a system with three-tire authentications. This system starts with registration of banking activities. The user of this bank must get registered and during the process of registration at the bank their fingerprint and mobile number will be gathered by banking staffs. Once the user wants to do a transaction, he/she must use the card and needs to provide the pin number. Once it is correct it moves to second step of verification, in the second step need to use finger prints. If it matches with bank database, an OTP will be sent to the user's mobile phone which they can use to make the transaction process. This is comparably more secure than other models

meanwhile very complex and time consuming activates. It is impossible to thieves to make theft in this method (Onyesolu & Okpala, 2017).

Kennedy Okokpujie et al used a system with finger print and GSM feedback model. In this system a user needs to register to the bank account and wants to give the fingerprint to particular bank. The banks will give an s-code (secret code) for the specific user. When the user wants to access the ATM he/she want to enter the pin number of ATM card then it moves to the second step verification. In second step there are two ways. In first way user must use fingerprint, if that match with database then able to do transaction. If fingerprint not work in case of some issues then user must enter s-code to the ATM and it will send OTP to user's phone, using that able to do the transaction process. If s-code is wrong then ATM account will be blocked. It could be noticed that if they do not use fingerprint, there is an alternative option which helps in emergency situations. One of the reliable persons can use this system and also in case of the theft activities, this system again asks two way verification using OTP, thus system would be secure enough and this model is better solution for ATM and Banks(Okokpujie, Olajide, John, & Kennedy, 2016).

G. Renee Jebaline, and *S. Gomathi developed a system called "*A Novel Method to Enhance the Security of ATM using Biometrics". In this system client needs to create an account in particular bank. While creating that account fingerprint image of the client would be taken by the bank and there is a number will be given by the specific branch of the bank due to reduce the network traffic and easy retrieval of accounts details from database of the system. Whenever client use the system they need to use their fingerprints to start the system, when the fingerprint is scanned by the system, it encrypts and while comparison process it decrypts and compares with already stored image from database, once both match, it allows the banking activities and if they want the statement about their bank detail they could use the number which has been given by the branch and can be fetched it. In addition to this, banker gets the client's ten fingerprints with their spouse hence in case of emergency spouse also able to access the system without any inconvenience (Jebaline & Gomathi, 2015).

Ossama H. Embarak implemented a system called "A two-steps prevention model of ATM frauds communications" for providing security to the ATM. In this system, whenever bank customers insert the card into ATM it will ask the pin number if he/she enters correct pin it will move to second step, in second step it will ask user to select either barcode or transaction pin number. If user selects barcode then bank system will generate the barcode by using hashing function which is a combination of Smart phone ID and some random number, once user gained that barcode then ATM ask user to display that barcode if it is matched then transaction will take place, else it rejects the transaction. Meanwhile if user selects transaction pin number, the bank system will follow same protocol by sending hash function, which also combination of smart phone ID and some random number, once user gets that number and if he/she enters correct pin then transaction will happen as usual. Here Smart phone act as major role for hash function process(Embarak, 2018).

Rasib Khan et al, developed a framework for ATM security called "SEPIA". This system relays on three major entities namely, SEIPA server, ATM and user of the system. Here user of the system needs to use wearable device like Google glass or other appropriate devices for avoiding the theft of card pin numbers and need to have a smart phone for login into the SEPIA server. This system initiates by touch the ATM screen by the user of the system. Once the system initiated, ATM sends transaction request message to the SEPIA server with request id and location id, when the server received request from ATM, It will prepare and generate transaction id and complicated numeric template or pin template for transaction process then it will send the same to the ATM with short time period of validity. Here pin template contains pin number to the ATM with some hidden numbers, for an instance, in case of 10-digit pin number it will send only five numbers and user must be fill that remain five number when he/she get the code from other procedure. Once ATM received the response from server, it will extract the transaction id and generate QR (Quick Response) code. The user of the system is able to see the QR code in ATM and he/she could be used the wearable device or mobile device for running SEIPA application to scan QR code. Once scan is finished, transaction request message of the user has been created and sent to the SEIPA server, this message contains location id,

request id and transaction id, username and password. When the SEIPA receives the request message from user wearable device or phone, it will verify and respond to user's device. Once it sends remaining number from SEIPA server, user of the system can fill the remaining hidden code and can start the transaction(Khan, Hasan, & Xu, 2015).

Chen Li et al, developed a system called "Human Body and Face Detection based Anti-shoulder Attack System on ATM" for mitigating shoulder surfing attack. In this system they have monitored ATM nearby person's body and face by using Gaussian Mixture Model (GMM) algorithm and AdaBoost-based algorithms respectively. Once they detect body and face, it will be combined together at "decision layer fusion", the layer already trained with shoulder surfing attack and if that found any unwanted activities then warning user to pay attention to that environment (Li et al., 2017).

M.Padmavathi and R.Nagarajan developed a lab view or simulation system for ATM called "Smart Intelligent ATM Using LABVIEW" for deliver protection against ATM frauds. In this system instead of using pin card they had used biometric fingerprint for transaction activities. This system consists of a PIC microcontroller which connected with fingerprint module, buzzer, LCD display and power supply. Whenever any customer enters into the ATM, they need to use the ATM card for user identifications, when the card is ok with identification he/she needs to use thumb for biometric verification, if it matches then transaction happens. If not buzzer will alarm to the environment (M.Padmavathi & R.Nagarajan, 2017).

Shweta Sankhwar and Dhirendra Pandey developed a way of mitigating the ATM fraud called "A SAFEGUARD AGAINST ATM FRAUD". In this method they used pin number and OTP for second step verification. Whenever user enters the ATM, he/she needs to use ATM card with pin number, if the pin number is correct then the Bank will send the OTP to the user's phone. To get OTP user must register the SIM card number when user opens the account. Once they apply the correct OTP then they proceed with the transaction. In here there is a threshold amount of cash withdrawal will set by the bank according to the user's wish. Whenever users withdraw less than or equal to threshold value then they don't need to use OTP, if the value is more than threshold they must use OTP for second verifications (Sankhwar & Pandey, 2016).

5. ATM Robberies Review

Sudipta Maiti et al recommended a security framework for forestalling ATM theft "Burglary insurance with GPS and Sensors". This framework acting with the assistance of two sensors and GPS. First sensor is placed at the passage entryway of the ATM which forestall more than one client section inside ATM. The other sensor is placed inside the ATM which additionally have two sub sensors in it specifically, vibrate and motion sensors which sense the harm or any undesirable issues in ATM and GPS will send the directions to the specific ATM to the responsible people in the event of any awkward entry or different issues occurred in ATM (Maiti, Vaishnav, Ingale, & Suryawanshi, 2016).

G.NAGADEEP and K.SAMBA SIVA RAO developed a system called "ADVANCED ANTI THEFT ATM SECURITY SYSTEM WITH ZIGBEE AND GSM" for prevent ATM Robberies. In this system they have used PIC microcontroller as intermediate device and, Vibrate sensor, IR Sensor, GSM module, Zigbee as an input and buzzer, LCD and Gas sensor act as output devices. Whenever more than one person enters the ATM, vibration sensor detect that events and sends to microcontroller then buzzer sound will be activated by the response from microcontroller, once the buzzer activated ATM gate will be closed with the help of DC motor and GAS will leak by stepper engine in addition, there is a SMS text will be sent to the authorized stakeholders like police and Bank staffs with the help of GSM module. And also, there is a SD card also used in the system for constant monitor of changes of sensor data. To identify more than one person enter into an ATM they had used PIR sensor with some calculation and vibrate sensor with weigh and speed activities(NAGADEEP & RAO, n.d.).

R.Kayalvizhi et al designed a concept called "anti-theft ATM robbery detection using big surveillance video data" for preventing from ATM Robberies. Whenever user enters the ATM, camera will start to monitor the user. If the user finishes the work within particular time period it just monitors the user and records the footage, if the time increases then, the camera will monitor the awkward

behaviors or irrelevant behaviors. When it finds any irrelevant activities like ATM robbery, then it will send the alert to responsible person. Here they have trained the camera to observe all irregular actions of the system by appropriate algorithms hence it identifies the illegal activities. Whenever the camera records the footage it follows necessary operations and send SVM classification, this classification compared with training phase which include irrelevant behavior and session time. Once this SVM classification match with training phase then it automatically send pre-alert to responsible person(Kayalvizhi, Kuil, & Saranya, 2019).

Sonali T. Saste and Prof. S. M. Jagdale developed a system for prevent ATM robbery called "Emotion Recognition from Speech Using MFCC and DWT for Security System". The system is working based on basic emotions like angry, happy, scared and neutral states. All emotions of ATM customer have been observed using microphone. Whenever customer of the bank speaks then feature extraction will collect by two algorithms called MFCC and DWT. Once the feature extraction collected it will be combined together and to classify emotion, SVM classifier has been used. Once the feature extraction concatenated result combined with SVM and it will decide the type of emotion and the necessary actions will be made by the responsible authority(Saste & Jagdale, 2017).

Raj M and Anitha Julian developed a system called "Design and implementation of anti-theft ATM machine using embedded systems" for preventing robberies in ATM. This system encompasses a RFID reader and RF transmitter placed outside with a raspberry pi Microcontroller and ATM is placed bit apart from the microcontroller. The ATM is designed with a Shutter Locking door, Camera, Buzzer, Vibrate sensor, Smoke sensor, Thermocouple sensor and RF receiver. Whenever user wants to enter the ATM he/she need to use the RFID tag placed in the microcontroller, once it reads the tag, login interface of the microcontroller check the tag with database details, if it matches, then RF transmitter transfer the signal to RF receiver placed in the ATM, once it received the correct signal shutter door open automatically with the help of DC motor. Then the users are able to enter ATM and can do their transactions. In case of heist activities like cutting, damaging and drilling, The vibrate sensor detect that activity and Smoke sensor release gas and shutter will be locked, buzzer will alarm to public meanwhile the message will pass to the near police station hence robberies mitigate considerably (Raj & Julian, 2015).

Ms.V.H.Kambale et al, developed a simulated system using Proteus and MPLAB called "ATM Crime Prevention System" for preventing ATM from physical attacks like Robberies. This system contains Piezo sensor, PIR sensor and microphone inside the ATM. Piezo sensor used for detecting any unwanted action like damaging, drilling by measuring pressure, acceleration, temperature, strain and convert those into electrical charge. PIR used for checking the changes of human body and microphone will inform the unusual incident to responsible person. Whenever any unexpected events happen as long vibration, uneven motion and screaming sound inside the ATM, then sensor detect those activities and sends the information to appropriate authorities with the help of GSM module and buzzer will be screaming the alert alarm hence the ATM user or bank can be protected (Kambale, 2018).

Bharati M Nelligani et al, proposed a high tech system called "Smart ATM Security System Using FPR, GGM, GPS" for mitigate robberies and ATM password hacking. In this study there is a PIC microcontroller used as an intermediate device and RFID reader, GSM, Camera, IR sensor, GPS and fingerprint module connected with that microcontroller as input and Buzzer, LCD, and Relay with shutter connected as output device and RFID used as an ATM card. Whenever user enters into ATM, he/she needs to swipe the RFID tag, once the id matches with database then the person needs to use his/her fingerprint, when it okay there is an OTP will be sent to the person's phone. The transaction can be completed using the OTP provided. GSM module is being utilized to send the OTP. If anyone try to damage the ATM, there is a shutter will be closed with the help of DC motor placed in the relay and message will pass to the accountable person and also buzzer will alarm to surrounding. If anyone take the cash box outside then location will send to the police with the help of GPS hence it is a challengeable system for heist (Nelligani, Reddy, & Awasti, 2016).

S.Shriram et al, developed a system called "Smart ATM Surveillance System" for providing fortify the ATM from robberies. ATMEGA-328 microcontroller as an interface between input and output. Temperature sensor, PIR sensor, accelerate meter and GSM module pretend as input of the microcontroller and LED, Siren and Shutter door with motor act as output device. Whenever customer of the bank enters the ATM, they can do their work without any obstacle. If any loot operation is observed by particular sensors it inform to microcontroller, as soon as it get the response from input, then the siren will alarm and the door shutter will be closed concurrently there is a message will be passed to the response person using GSM module (Shriram, Shetty, Hegde, Nisha, & Dharmambal, 2016).

Vishal Sanserwal and Vikas Tripathi developed an ATM abnormal protection method using CCTV called "Comparative Analysis of Various Feature Descriptors for Efficient ATM Surveillance Framework". This system fully relies on videos from CCTV camera and, the video footage is converted to frames. The feature extraction will happen to these frames using HOG, Zernike moments, Hu Moments and their different combinations to obtain motion features in the image sequence. After that, there is a method called Random forest Classifier used to identify whether the activity is abnormal or not. When the result is normal transaction will take place else it blocks the transaction and alert the responsible stakeholder (Sanserwal, Pandey, & Chen, 2017).

Sambarta Ray et al developed a system called "An Intelligent Vision System for monitoring

Security and Surveillance of ATM" for mitigate robberies. In this system there is a camera placed at the ATM and it will capture the individual frames whoever enter the ATM. While it recording it does two things. First its analysis the number of people enter the ATM, when the amount is higher than particular amount it will send warning message to authorities. Second it checks whether any person using any mask, if so, it sends warning message. To identify the frame and face they have used Viola-Jones algorithm (S. Ray, 2015).

6. Methodology

The Major objectives of this studies are; 1) Implement a three-factor ATM heist prevent method using Pin, OTP or Fingerprint and Pattern Lock 2) Review the previous studies relevant to this study and recommend a solution based on implementation and comparison.

7. System Architecture

Figure 2 shows the flowchart of three factor Authentication of ATM. Initially user of the system needs to use their ATM card for pin verification, once that pin matches with database, system moves to second verification, if not they can try up to 3 times. In second phase ATM will ask the user's option to select whether it is OTP or Fingerprint. When user selects OTP, then the system sends the OTP to the user's Smartphone. If OTP matches, then user needs to go for final verification. If the user selects fingerprint, they want to place their thumb to the fingerprint interface, if it is matches with database then they are allowed for final verification, if not they can try up to 2 times. In 3rd phase user needs to draw a pattern to ATM screen which they already given to the bank. If the pattern mismatches with database more than two times then ATM halts the card for security purpose. If user draws correct pattern with database details, then users are able to do their transaction process without any delay.

7.1. System Components and software tools

- **OTP**: One Time Password Used in mobile devices for second verification process(Erdem & Sand\ikkaya, 2018).
- **Pattern Lock**: It is a type of password authentication mechanism used in mobile and other smart devices for prevent unauthorized access (Zhou et al., 2018).
- **Javafx**: Library used to create rich and smart GUI and Web based application (Chin, Vos, & Weaver, 2019).

- **Scene Builder**: Software Application used for Build UI component which helps to build javafx applications (Vos, Chin, Gao, Weaver, & Iverson, 2018).
- **Database**: Collection of table which allows to store data (Narang, 2018).
- **MySQL Workbench**: Software tool allow us to handle database relevant activities (Krogh, 2020).

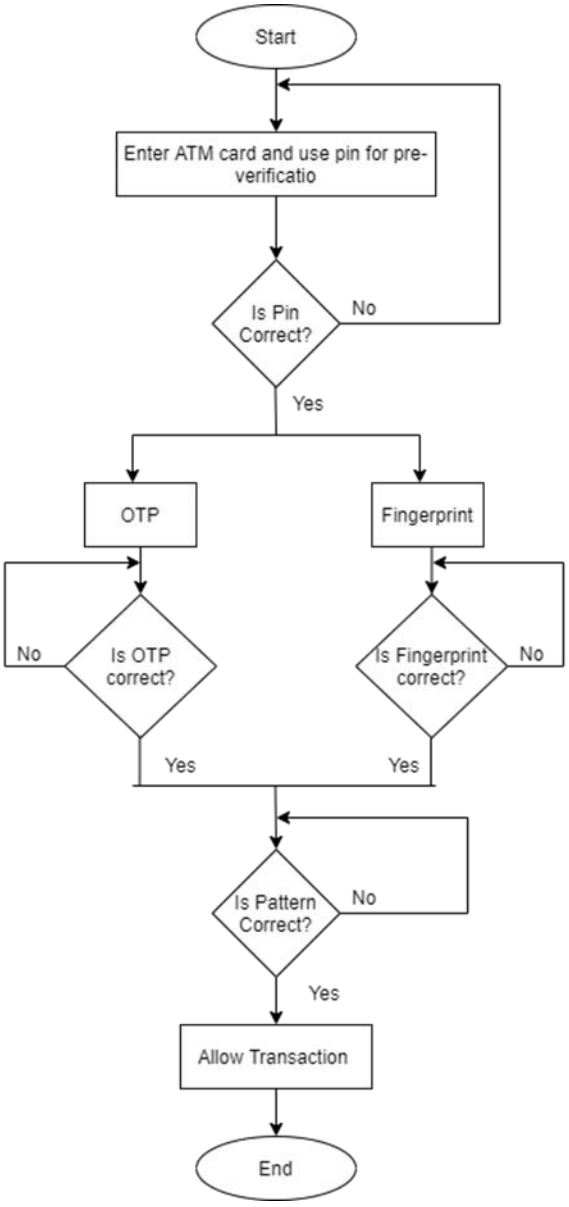


Figure 2: Flow Chart for Three factor System

8. Result And Discussion

8.1. Result and Discussion for three-factor Authentication

Figure 3 and Figure 4 show the database schema and stored data respectively. It is obvious from Figure 4 that, 1212 for pin number, +447418312638 as phone number and pattern stored as 1,0,0,0,0,2,3,0,0 which indicates “V” shape in 2D array.

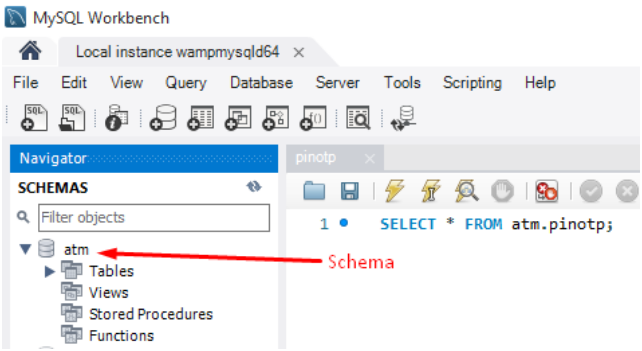


Figure 3: Workbench Database Schema

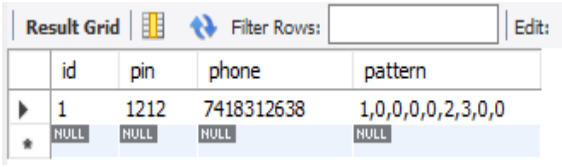


Figure 4: Database Data

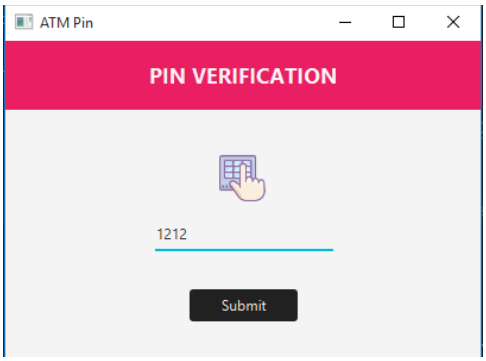


Figure 5 Pin Verification Interface

Figure 5 shows the Graphical user interface for entering pin Number to the ATM. Here 1212 pin number has added in the text field as in the database. Once user enters the correct pin number and click the submit button it moves to second verification. Here pin number is visible due to the demonstration purpose and when we use password field it becomes invisible. Figure 6 shows the options to the second verification process, in this phase user can either select OTP or they can go with Fingerprint. Based on their intention of easiness they can select the appropriate option. When the user selects the OTP, they will interact with following user interface, Figure 7 shows the Alert Dialog box for informing that OTP has sent. Now user of the system can be obtained the OTP message via phone number and able to finish the second step verification. Figure 8 shows the coding part for sender's name (Here mentioned as "ATM_TEAM") and OTP message. When user gets the message, it displays sender as "ATM_TEAM" and that message contains "Your OTP is :< OTP Number > ".

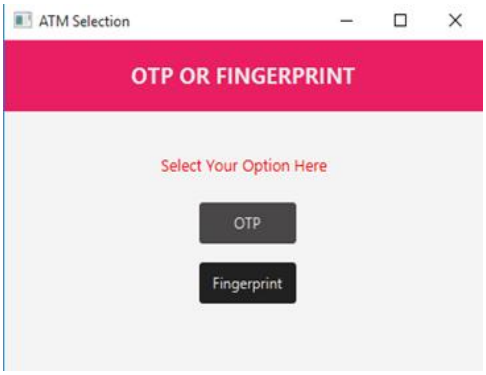


Figure 6: Option to second verification

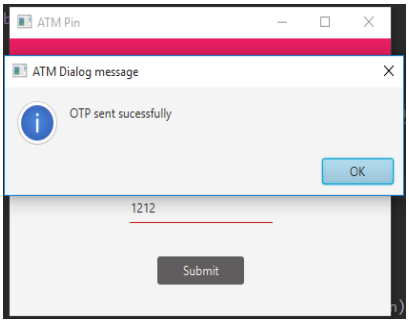


Figure 7: OTP Alert Dialog Message

```
String message = "&message=" + "Your OTP is : "+OTP;
String sender = "&sender=" + "ATM_TEAM";
```

Figure 8: Name of the sender and OTP message

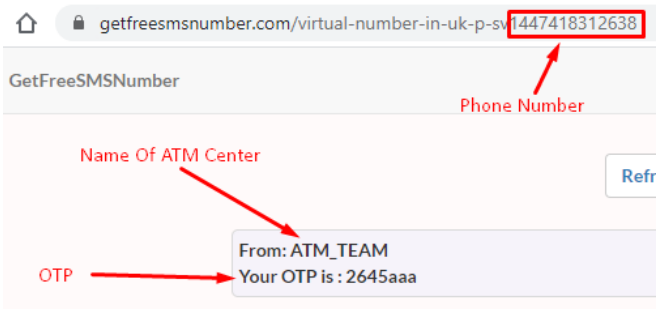


Figure 9: OTP message to Phone

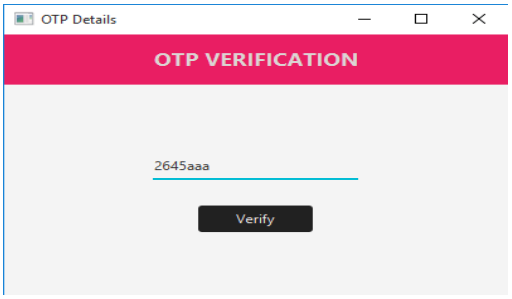


Figure 10: OTP Verification Interface

Figure 9 and Figure 10 shows the obtained OTP message to the phone number and OTP verification interface respectively. In Figure 9, it clear that sender and message are same as mentioned above. Here we used virtual phone number for getting the message due to the API we selected and security purpose. Also, Text Field used to demonstrate that, what we are typing in the OTP verification interface. Once it is okay then user needs to move to third verification process of Pattern Identification. Meanwhile if the user selects finger print, they will interact with following interface.

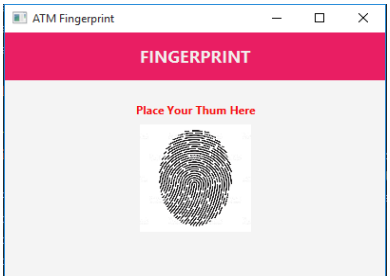


Figure 11: Fingerprint thumb interface

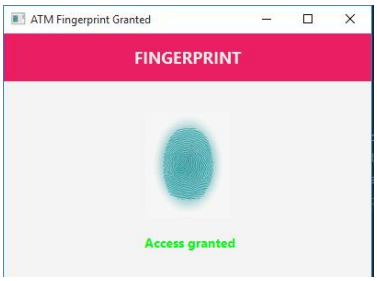


Figure 12: Access is granted interface

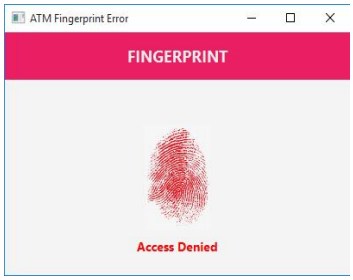


Figure 13: Access is Denied Interface

```
1  CREATE TABLE `atm`.`fingerprint` (
2    `id` INT NOT NULL,
3    `Name` VARCHAR(45) NOT NULL,
4    `Image` LONGBLOB NOT NULL,
5    PRIMARY KEY (`id`));
6
```

Figure 13: Access is denied interface

Figure 14: Database Table of fingerprint

Figure 11, 12, and 13 show fingerprint thumb, access is granted, access is denied interface individually. Whenever user choose fingerprint option from figure 6, they will interact with figure 11 and they need to use their thumbs for second step verification, once it matches with database stored image, interface change as figure 12 and if not, it become as in the figure 13. As soon as it matches with database it moves to 3rd phase pattern verification. Figure 14 and 15 shows the fingerprint table and user's image data which is stored in the database in MySQL workbench. Figure 16, 17 and 18 shows the Pattern Lock interface, Matched password with Database as well as wrong pattern password which mismatches with database. When the user enters into this step, they need to draw the correct pattern. If its correct user can do their transaction activities and if it fails more than two time, they are unable to do it.

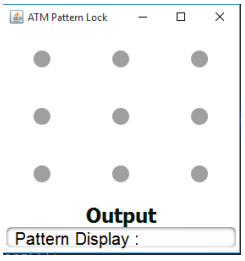


Figure 16: Patter Lock Interface

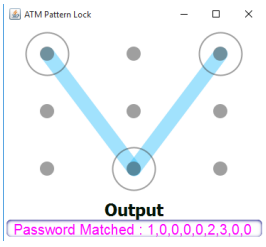


Figure 17: Matched Password

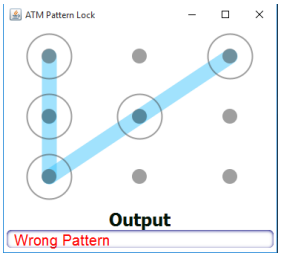


Figure 18: Wrong Password

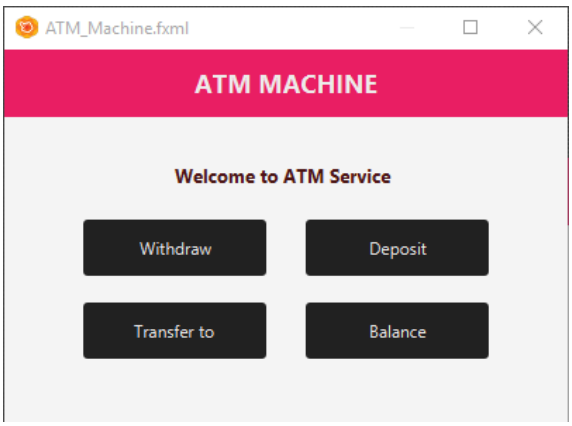


Figure 19: ATM Service Interface

When all those three activities done successfully user can do the transaction using this Interface.

8.2. Prototype testing of three factor ATM system

Before the real utilization of our suggested security tiers in ATM, our system needed to be evaluated. To evaluate our suggested security tiers in ATM, the prototype of our suggested system was developed and tested with 400 university students. Through the evaluation process, the accuracy and the performance of the system was evaluated. The result of the evaluation attested that the suggested security tiers could be implemented in the real environments and can be used to overcome the security threats which is being faced in current ATM security system.

Table 1 Result of prototype test

Tiers	**Security types**	**Success**		**Failure**	
		Number	**Percentage (100%)**	**Number**	**Percentage (100%)**
01	Pin (400)	384	96	16	04
02	OTP (160)	151	94.375	09	05.625
	Fingerprint (224)	212	94.64	12	05.357
03	Pattern (363)	360	99.17	03	0.83

Table 1 describes the result of the evaluation of the prototypes of our suggested security tiers to overcome the security issues faced by ATM users. As mentioned earlier, total 400 university students participated in the evaluation process. As our initial security tier is entering security pin, the selected 400 students were allowed to enter their security pin into our developed porotype. And the 384 users entered correctly for first time, but 16 users got failed to enter correct security pin. As the result of our prototypes, the performance of the first tier is 96%. For the second tier, the users who got pass in the first tier (384 students) allowed to choose one option out two options which is OTP and Fingerprint. OTP had been chosen by 160 users and 224 users chosen Fingerprint. Of those who reported OTP, 151 were successful and the percentage of success is 94.375%. The 05.357% of users got failed in OTP

option, because of they did not get the OTP number in their phone, due to mobile network coverage problem.

Of those who reported Fingerprint, 212 were successful and the percentage of success is 94.64% and the percentage of failure is 05.357%. The result of the second tier indicates that most users selected Fingerprint option to avoid difficulties faced in OTP process. And the success rate also high in Fingerprint option. Of those who got succeeded in the both second security tiers which is OTP and Fingerprint (363 students), allowed to our final security tier which is Pattern. Out of 363 users, the 360 got succeeded and the percentage is 99.17%. Only 0.83% users got failed which is 03 in number. The result of tier 3 shows that, remembering pattern is easy and high secure as well. When we see the overall result of this evaluation process, our suggested security tiers are applicable and accuracy in performance as well. Therefore, the suggested security tier is the way to overcome the security problems which are being faced in current ATM security system.

8.3. Comparison and Discussion for Systematics Review

Table 2: ATM Heist Security System from previous studies

ATM Card Heist Security Systems	**Available security methods**						
	Pin	**OTP**	**Biometric**	**Barcode & Transaction id**	**Algorithms**	**Quick Response code**	**Wearable devices**
A Novel Method to Enhance the Security of ATM using Biometrics	x	x	✓	x	x	x	x
A two-steps prevention model of ATM frauds communications	✓	x	x	✓	x	x	x
SEPIA	✓	✓	x	✓	x	✓	✓
Human Body and Face Detection based Anti-shoulder Attack System on ATM	x	x	x	x	✓	x	x
Smart Intelligent ATM Using LABVIEW	✓	x	✓	x	x	x	x
A safeguard against ATM fraud	✓	✓	x	x	x	x	x
Fingerprint and GSM feedback model	✓	✓	✓	x	x	x	x
Three-tire ATM authentications System	✓	✓	✓	x	x	x	x
Two-way ATM verification system	✓	x	✓	x	x	x	x
Palm Vein Biometric Technology	x	x	✓	x	x	x	x
Working with one time password (OTP) and facial recognition features	x	✓	✓	x	x	x	x
Security system for ATM by using Biometrics and OTP	✓	✓	✓	x	x	x	x

- Fingerprint and GSM feedback model – either fingerprint or OTP, when fingerprint okay there is no need of Biometric. If they go other way around, vice versa
- Security system for ATM by using Biometrics and OTP – Here 2nd verification user either may go with OTP or Facial recognition. Based on their comfort level they may choose the option.
- Biometric – Fingerprint, Facial, Retina

Table 2 shows the most recent systems concerning the ATM heist protection and the technologies which helps to give defense from theft heists. This table obviously and clearly shows that, most systems run with pin, OTP and Biometric and very few systems work with other techniques. Generally, users of any system prefer that, working system must be less complex, user-friendly, easier to use and it must not provide irritation while working on the system. In that respect, Tree-tire or Two-tire security is okay when considering from user view meanwhile we are living in a digital era anything is possible, still two or three layer we cannot assure the security and we need some modification. From above table 1 it clear that, "SEPIA" system relatively has more security measures than other all system hence SEPIA is one of the best systems among all ATM heist systems. Also, the working procedure of SEPIA is user-friendly, easy to use and it is not complex. If the user is okay with google glass they can afford and use without any hesitation, if not they can deal with smart phones. This system meets the general user comments and the security procedures. Hence, we are able to recommend this system for used any ATM to protect from any ATM heist.

Table 3: ATM Security Methods and provided solution from ATM fraud

ATM Security Methods	**Attack and measure / Solutions**		
	Shoulder Suffering	**Skimming**	**Hidden Cameras**
OTP	x	x	✓
PIN	✓	✓	✓
Biometric	x	x	✓
Google Glass	x	x	x
QR Code	x	x	✓

Table 3 shows the possible security methods against the current trend of ATM fraud methods.
- Indicates possibilities of attack
x - Indicates protection against the attack.

Most ATM security methods of table 3 have possibilities to attack by the Hidden Camera but Google Glass not allowed that attack and also Even though frauds can be monitored the OTP with hidden camera, that is useless for them due to the changing number of pin each time. From the above table Google Glass and OTP are somewhat security methods from other methods.

Table 4: Robbery Protection System

Robbery Protection Systems	**Modules and Sensors**
Robbery protection with GPS and Sensors	GPS, Motion and Vibrate Sensor
advanced anti-theft ATM security system with Zigbee and GSM	Vibrate sensor, IR Sensor, GSM module, Zigbee, buzzer, LCD, Gas sensor, DC Motor, SD Card and Pic Microcontroller
anti-theft ATM robbery detection using big surveillance video data	Camera, SVM classification (Image processing Technique), alarm
Emotion Recognition from Speech Using MFCC and DWT for Security System	Microphone, SVM(MFCC and DWT), alarm
Design and implementation of anti-theft ATM machine using embedded systems	RFID Reader, RF transmitter, Raspberry pi microcontroller, Camera, Buzzer, Vibrate sensor, Smoke sensor, Thermocouple sensor and RF receiver
ATM Crime Prevention System	Piezo sensor, PIR sensor, microphone, GSM Module,

	Buzzer
Smart ATM Security System Using FPR, GGM, GPS	RFID reader, GSM, Camera, IR sensor, GPS, fingerprint module, PIC microcontroller, LCD, Buzzer, Relay, DC motor
Smart ATM Surveillance System	Temperature PIR sensor, Accelerate meter, GSM module, LED, Siren, Shutter door, DC motor, ATMEGA-328 Microcontroller
Comparative Analysis of Various Feature Descriptors for Efficient ATM Surveillance Framework	Image processing Technique and alarm
An Intelligent Vision System for monitoring Security and Surveillance of ATM	Camera with image processing and alarm

Table 3 shows both IoT sensor techniques and Image processing techniques to identify the ATM Robbery. Normally this kind of system expects as real-time alarm system dealing with responsible person, GPS coordinate to the exact location and it must be cheap when compared with other system. In that respect "Advanced anti-theft ATM security system with Zigbee and GSM (A)" and "Smart ATM Security System Using FPR, GGM, GPS (B)" are somewhat met the criteria. The special of these systems when compared with others are auto-locking ATM door system with the help of DC motor so robber cannot be escaped once entered into it. Also these systems A and B have GPS and GSM module functions hence message will pass on-time while alarming and both using Pic Microcontroller with some sensor thus it cheap as well. When compare with A and B, A is best because it holds Gas sensor with locking door so robber will get faint when enter the ATM room but B doesn't have this facility.

Table 5: Sensors and Functions

Sensors	**Detection or Functions**
FSR(Force sensitive sensor)	Motion, Heat, change in orientation (Malvade, Joshi, & Madhe, 2017)
IR Sensor	Heat (P. P. Ray, 2017)
PIR	Motion (Sahoo & Pati, 2017)
Piezo	Pressure, Acceleration, Temperature, Strain(Kashimoto, Fujimoto, Suwa, Arakawa, & Yasumoto, 2016)
GPS	Position, Timing (Sun, Chang, & Chen, 2015)
Vibrate	Velocity, Displacement, Acceleration(David, Muthukumar, Ayyappan, & Ravi, 2020)
Gas	Existence or Concentration of gas(Kou et al., 2018)
Thermocouple	Temperature(Markevicius et al., 2018)

Table 6: Price of Microcontroller Board

Microcontroller	**Price**
PIC	Rs. 70 ("Pic Microcontroller Price," n.d.)
ATMEGA-328	Rs. 100 ("At Mega 328," n.d.)
Raspberry pi	Rs. 2355 ("Raspberry Pi Price," n.d.)

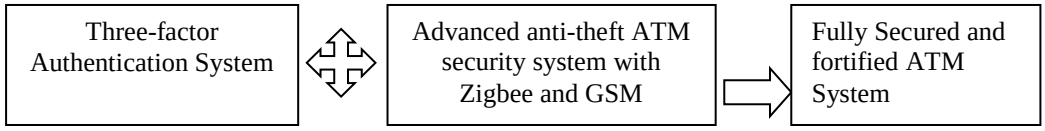
9. Conclusion

During the whole studies we are able to point out and identified very important and interesting points. To protect an ATM, Banks need to give both, card heist protection via standard software and Physical

protection for fortify the banks against robberies. To overcome the ATM heist problems two-factor verification is somewhat okay rather than only going with pin number. If they switch three-factor certainly heist problem will be very less most of the time. "SEPIA" method is one of the best ATM heist method among all but when we considering the cost issue two or three factor is fine. Biometric verifications also made major roles in additional verification process**.** Robberies site nowadays focus on Image processing and IoT Techniques. Robberies are very important problem almost every place all over the word. To overcome this issue, need implement and follow high security measures and protocols. "Advanced anti-theft ATM security system with Zigbee and GSM" one of the best security methods among all these analyses and if we implement a security protocol along with this method surely reduce ATM robberies considerably.

Recommendation

Normally an ATM needs security protocol for protecting against card heist and robberies. In this study we have implemented only card heist software system. Still we need to focus on physical robbery site. With this three-factor authentication system, when we merge "Advanced anti-theft ATM security system with Zigbee and GSM" system, it becomes one of best security system which handle both problems.



Reffere nce

[1] Bhosale, S. T. (2014). S ECURITY I N E-B ANKING V IA C ARD L ESS B IOMETRIC, (March).

[2] Chin, S., Vos, J., & Weaver, J. (2019). JavaFX Fundamentals. In The Definitive Guide to Modern Java Clients with JavaFX (pp. 33–80). Springer.

[3] David, A., Muthukumar, A., Ayyappan, D., & Ravi, S. (2020). Accident Avoidance System by Using Sensors Module. Test Engineering & Management, The Mattingley Publishing Co., Inc. ISSN, 193–4120.

[4] Embarak, O. H. (2018). A two-steps prevention model of ATM frauds communications . 2018 Fifth HCT Information Technology Trends (ITT), (Itt), 306–311. https://doi.org/10.1109/CTIT.2018.8649551

[5] Erdem, E., & Sand\ikkaya, M. T. (2018). OTPaaS—One time password as a service. IEEE Transactions on Information Forensics and Security, 14(3), 743–756.

[6] Hamid, M. (2015). Securing ATM with OTP and Biometric. International Journal on Recent and Innovation Trends in Computing and Communication, 3(4), 2041–2044. https://doi.org/10.17762/ijritcc2321-8169.150460

[7] Hodges, W. A. (2018). ATM skimmer detection based upon incidental RF emissions. Google Patents.

[8] Jebaline, G. R., & Gomathi, S. (2015). A novel method to enhance the security of ATM using biometrics. IEEE International Conference on Circuit, Power and Computing Technologies, ICCPCT 2015, 2–5. https://doi.org/10.1109/ICCPCT.2015.7159391

[9] Kambale, M. V. H. (2018). Atm crime prevention system, IV(2350), 5–7.

[10] Karovaliya, M., Karedia, S., Oza, S., & Kalbande, D. R. (2015). Enhanced security for ATM machine with OTP and facial recognition features. In Procedia Computer Science (Vol. 45, pp. 390–396). Elsevier Masson SAS. https://doi.org/10.1016/j.procs.2015.03.166

[11] Kashimoto, Y., Fujimoto, M., Suwa, H., Arakawa, Y., & Yasumoto, K. (2016). Floor vibration type estimation with piezo sensor toward indoor positioning system. In 2016 International

Conference on Indoor Positioning and Indoor Navigation (IPIN) (pp. 1–6).
[12] Kayalvizhi, R., Kuil, M. T., & Saranya, M. (2019). ANTI-THEFT ATM ROBBERY DETECTION USING BIG SURVEILLANCE VIDEO DATA, 1(1), 31–34.
[13] Khan, R., Hasan, R., & Xu, J. (2015). SEPIA: Secure-PIN-authentication-as-a-service for ATM using mobile and wearable devices. In Proceedings - 2015 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering, MobileCloud 2015 (pp. 41–50). https://doi.org/10.1109/MobileCloud.2015.16
[14] Kibona, L. (2015). Face Recognition as a Biometric Security for Secondary Password for ATM Users . A Comprehensive Review. Ijsrst |, 1(2), 1–8.
[15] Kou, X., Xie, N., Chen, F., Wang, T., Guo, L., Wang, C., … others. (2018). Superior acetone gas sensor based on electrospun SnO2 nanofibers by Rh doping. Sensors and Actuators B: Chemical, 256, 861–869.
[16] Krogh, J. W. (2020). MySQL Workbench. In MySQL 8 Query Performance Tuning (pp. 199–226). Springer.
[17] Kumar, M. (2014). Tyupkin Malware Hacking ATM Machines Worldwide.
[18] Li, C., Liang, M., Xiao, K., Fong, S., Wang, Q., & Song, W. (2017). Human Body and Face Detection based Anti-shoulder Attack System on ATM, 2–5.
[19] Lija, J., & Santo Varghese, S. (2017). An Advanced Digitalized System to Resist Shoulder Surfing Attacks in ATM. Central Library.
[20] M.Padmavathi, & R.Nagarajan. (2017). Smart Intelligent ATM Using LABVIEW, 5(5), 41–45.
[21] Maiti, S., Vaishnav, M., Ingale, L., & Suryawanshi, P. (2016). Atm Robbery Prevention Using Advance Security, 1022–1024.
[22] Malvade, P. S., Joshi, A. K., & Madhe, S. P. (2017). IoT based monitoring of foot pressure using FSR sensor. In 2017 International Conference on Communication and Signal Processing (ICCSP) (pp. 635–639).
[23] Markevicius, V., Navikas, D., Andriukaitis, D., Cepenas, M., Valinevicius, A., Zilys, M., … Idzkowski, A. (2018). Two thermocouples low power wireless sensors network. AEU-International Journal of Electronics and Communications, 84, 242–250.
[24] NAGADEEP, G., & RAO, K. S. S. (n.d.). ADVANCED ANTI THEFT ATM SECURITY SYSTEM WITH ZIGBEE AND GSM, 3(2), 106–111.
[25] Narang, R. (2018). Database management systems. PHI Learning Pvt. Ltd.
[26] Nelligani, B. M., Reddy, N. V. U., & Awasti, N. (2016). Smart ATM security system using FPR, GSM, GPS. Proceedings of the International Conference on Inventive Computation Technologies, ICICT 2016, 2016. https://doi.org/10.1109/INVENTIVE.2016.7830093
[27] Okokpujie, K., Olajide, F., John, S., & Kennedy, C. G. (2016). Implementation of the Enhanced Fingerprint Authentication in the ATM System Using ATmega128 with GSM Feedback Mechanism.
[28] Onyesolu, M. O., & Okpala, A. C. (2017). Improving Security Using a Three-Tier Authentication for Automated Teller Machine (ATM), (October), 50–56. https://doi.org/10.5815/ijcnis.2017.10.06
[29] Oškrdalová, G. (2016). Payment Card Frauds with a Hidden Camera, Touch Sensors and a Counterfeit Payment Card and Protection Techniques against these Types of Frauds. European Financial Systems 2016, 526.
[30] Pic Microcontroller Price. (n.d.).
[31] Prasanthi, B. V., Hussain, S. M., Kanakam, P., Chakravarthy, A. S. (2015). Palm Vein Biometric Technology : An Approach to Upgrade Security in ATM Transactions. International Journal of Computer Applications, 112(9), 1–5. https://doi.org/10.5120/19691-1440
[32] Raj, M. M. E., & Julian, A. (2015). Design and implementation of anti-theft ATM machine using embedded systems. In IEEE International Conference on Circuit, Power and Computing Technologies, ICCPCT 2015. https://doi.org/10.1109/ICCPCT.2015.7159316

[33] Raspberry Pi Price. (n.d.).
[34] Ray, P. P. (2017). An IR Sensor Based Smart System to Approximate Core Body Temperature. Journal of Medical Systems, 41(8), 123.
[35] Ray, S. (2015). An Intelligent Vision System for monitoring Security and Surveillance of ATM, 3–7.
[36] Sahoo, K. C., & Pati, U. C. (2017). IoT based intrusion detection system using PIR sensor. In 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT) (pp. 1641–1645).
[37] Sankhwar, S., & Pandey, D. (2016). A Safeguard against ATM Fraud. Proceedings - 6th International Advanced Computing Conference, IACC 2016, (June), 701–705. https://doi.org/10.1109/IACC.2016.135
[38] Sanserwal, V., Pandey, M., & Chen, Z. (2017). Comparative Analysis of Various Feature Descriptors for Efficient ATM Surveillance Framework, 539–544.
[39] Saste, S. T., & Jagdale, P. S. M. (2017). Emotion Recognition from Speech Using MFCC and DWT for Security System, 701–704.
[40] SEQUENCE DIAGRAM OF TRADITIONAL ATM PROCEDURE. (n.d.).
[41] Shriram, S., Shetty, S. B., Hegde, V. P., Nisha, K. C. R., & Dharmambal, V. (2016). Smart ATM Surveillance System.
[42] Singh, M., Ayub, S., & Verma, R. (2013). Enhancing Security by averaging multiple fingerprint images. In 2013 International Conference on Communication Systems and Network Technologies (pp. 487–490).
[43] Sun, J. C.-Y., Chang, K.-Y., & Chen, Y.-H. (2015). GPS sensor-based mobile learning for English: an exploratory study on self-efficacy, self-regulation and student achievement. Research and Practice in Technology Enhanced Learning, 10(1), 23.
[44] Vos, J., Chin, S., Gao, W., Weaver, J., & Iverson, D. (2018). Using Scene Builder to Create a User Interface. In Pro JavaFX 9 (pp. 129–191). Springer.
[45] Zhou, M., Wang, Q., Yang, J., Li, Q., Xiao, F., Wang, Z., & Chen, X. (2018). Patternlistener: Cracking android pattern lock using acoustic signals. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (pp. 1775–1787).