Trifecta Approach to ATM Transaction Security

Afia Farzana
Student, American International
University-Bangladesh (AIUB)
1408/1, Kuratoli, Khilkhet,
Dhaka 1229, Bangladesh

Noor Mohammad
Student, American International
University-Bangladesh (AIUB)
1408/1, Kuratoli, Khilkhet,
Dhaka 1229, Bangladesh

Sharif Ahmed
Student, American International
University-Bangladesh (AIUB)
1408/1, Kuratoli, Khilkhet,
Dhaka 1229, Bangladesh

Jannat Ara Mim
Student, American International University-
Bangladesh (AIUB)
1408/1, Kuratoli, Khilkhet, Dhaka 1229, Bangladesh

Juena Ahmed Noshin
Assistant Professor, American International
University-Bangladesh (AIUB)
1408/1, Kuratoli, Khilkhet, Dhaka 1229, Bangladesh

ABSTRACT
This is the twenty-first century and everything nowadays revolves around high-performance technology and its security. But there are numerous limitations in this security part and because of this we are facing adverse situation frequently. ATM transaction is one of the biggest inventions for this modern world because millions of people are using ATM for transaction purpose. But in ATM transaction people are facing many types of security issue and for this reason they are afraid for doing big amount of transaction from ATM. This paper works towards reducing this security problem. In our proposed system we are using two types of authentication. One is simple security authentication and another is strong security authentication. In simple security authentication there are two steps. First one is bank provided PIN and second one is entering the fingerprint. In strong security authentication there are three steps. First one is bank provided PIN, second one is location tracking and third one is a choice of option between fingerprint and OTP. There will be a time limit for OTP which is 40 seconds. Actually, our main focus is on strong security authentication. But for some time being we will also be giving the facility of using simple security authentication so that gradually people can be habituated with the strong security authentication. When using strong security authentication becomes a second nature, we will remove the simple security authentication from the system. By following the mentioned process, we are trying to solve the ATM transaction security issue.

General Terms
Cyber Security

Keywords
Automated Teller Machine, GPS, Fingerprint, OTP

1. INTRODUCTION
Automated Teller Machine (ATM) is a machine through which its users can get the service of money transaction anytime and anywhere. It is a computer-based machine through which users are handed out cash from bank without their physical presence because by using the account number any kind of transaction can happen. Also, this ATM machine can provide the service of money transfer from different bank accounts and some other elementary information such as: current cash amount, minimum and maximum money withdrawal amount etc. [1]. This machine is connected with electricity and network. ATM card transaction is the most frequently used technology in present times. One of the most convenient part of ATM transaction service is it gives 24-hour service to its users. Because of this ATM card, life is getting easier since people are now carrying a little amount of cash and doing almost every cash related task with ATM card. With the help of this ATM card people can do multiple tasks like they can pay the electricity bill, utility bill, food bill etc. Bank is another important part of our modern life and from this bank the service of ATM card is provided. This is because by using ATM service more, it is reducing the rush in banks and as there is a service charge for ATM card so banks can earn more money from this ATM service which is improving the business quality as well. Although the invention of ATM is giving a drastic and positive change in this world but the security purpose is not maintained in a fool proof way yet. The usual security system followed is that there is a PIN number of 4 digits which is provided by the built-in system from bank. User swipe their card in the machine and input the PIN in the machine, so if anyone can steal the card and the PIN number, they can easily get the access of money within a very short period of time. For this reason, many researchers are trying to improve on the existing approaches to ATM transaction security. In this paper we are also proposing a new security method for ATM transaction purpose using OTP and Fingerprint. For our security approach smartphone will be used so the chances of hacking password will be reduced to a great extent. The following is the format of this paper: In section 2 the literature review is discussed of other ATM security work related papers and the proposed model in [13] is explored thoroughly. In section 3 our proposed model is introduced which is a modified version of the proposed model in [13] aimed at resolving its existing limitations. Section 4 is about the advantages of our proposed model. Section 5 is about the comparison between previous work and our work.

The last section is 6 where conclusion is drawn of the whole concept.

2. LITERATURE REVIEW
Moses Okechukwu Onyesolu and Ignatius Majesty Ezeani [1] conducted a survey on ATM security using fingerprint biometric identifier. From last few years electronic transactions are having a higher growth all over the world and this transaction system also has a security system for the

safety of users. Normally users have a specific PIN which they use for transaction but they want faster and more accurate authentication because there is a high chance that anytime the PIN number can be hacked but if user use a biometric identifier like fingerprint, they can do their any type of transaction with much more safety and it also be a faster process. They said that there are many types of biometric identifier like face recognition, fingerprint, iris, signature, voice etc. but the percentage of fingerprint identifier as a security system for ATM is higher which is almost 62% than the others biometric system mentioned above and as 74% people have heard about fingerprint system before so it will be an easy process for users and they can also adopt this biometric process for ATM transaction quickly.

Sridevi Bonthu [2] proposed a system that help provide user a better security service at the time of ATM transaction. An approach is proposed in which a standard fingerprint scanner is combined with a DNA barcode generator. When opening a bank account, users must first have fingerprint impressions provided by a fingerprint scanner as well as DNA samples. DNA samples were sampled and processed before being translated to barcodes with the aid of a DNA barcode generator. The barcode obtained is added to the back of each person's ATM card. The fingerprint scanner must be connected to the ATM terminal while processing with it. When a customer attaches their ATM card and then puts their finger on a fingerprint scanner, the image of their fingerprint is captured. They assume that integrating finger print and DNA data provides more precise and consistent results than current approaches such as ATM access with fingerprint and GSM.

Srivatsan Sridharan et al, proposed [3], two tiers authentication for security purpose. They are using one-time Pass Key (PK) and Random Security Question (RSQ). One-time pass key will be provided by the system. The system will send a key to user phone number as a message. After entering the pass key, the machine server will generate some random security questions for user in the machine monitor. If the given answer is valid then user can successfully do their transaction.

According to [4], for more secure system in ATM transaction field, they are using biometric and GSM technology. In this process at the time of opening a bank account, bankers will collect the fingerprints and phone number of the user and will store it in the database system of that bank. When that user wants to do transaction at first level user will give fingerprint then it will be checked with the stored fingerprint in the database system that it is authenticated or not. If the fingerprint is not authentic then the GSM modem will send a message in the bank security department and if the fingerprint is verified then a message will be sent to the user's phone which is a 4-digit random pin. After getting the pin user will enter the pin and if it is correct user can do their task and if the pin is not correct then the system will terminate.

According to [5], there are two authentication system. One is for user and another is for admin. For user, when one user places the card in the ATM machine there will be two options, one is OTP and the other one is fingerprint. If user choose OTP, a pin will be sent to the registered phone number of that user then user need to enter the OTP in the system if OTP matched user can do their transaction. But when a user chooses fingerprint option, first user will enter their fingerprint in the machine, if the fingerprint matched there will be two mode one is for transaction and another one is for

admin because admin cannot do their transaction like user. After selecting transaction user can proceed further.

According to [6] to prevent unauthorized transaction and to prevent pin hacking they invented a new system using face recognition and OTP. They introduced that after card swiping there will be face recognition step. Through PCA software face will be recognized. If face is not recognized account will be blocked temporarily and if face is recognized properly, an OTP will be sent in customer's phone number. After entering that OTP in the system, it will track how many times customer is trying to enter OTP. If attempts cross more than three times system will block account temporarily and will notify the customer and if the attempts are less than three times and OTP is correct customer can do their transaction.

Michael Asante [7] proposed a system that can increase the overall security level of ATMs. They use multifactor authentication that means on a first security stage when user insert the card that time a random verification code sent to their registered number and user insert the given number in the ATM. If that works then they follow up to the next verification step that is fingerprint. Then user provide their registered finger to complete the all-necessary verification process. They went on to say that this system is a decent cost-effective way to enforce safe ATM transactions and shield ATM users from fraudsters.

In 2017, two students of Jahangirnagar University, Bangladesh introduced a new way of ATM transaction authentication using client's fingerprint. They proposed that after the insertion of ATM card in the machine clients have to put his/her finger in the fingerprint part. If the fingerprint is matched with stored fingerprint in the database system then in the client's registered mobile number a 4-digit code will be sent. After that the client need to enter the code in the ATM machine and then transaction will start. This whole process can be done within three successive attempts after three attempts client's account will be blocked for 24 hours and a message will be sent both to the respective bank and client's registered number [8].

In this paper [9], researchers used a multi-factor level for authentication system. They used an optimized Advanced Encryption Standard (AES) algorithm for security purpose. There are two level of security. First of all, client will give fingerprint as a biometric authentication then a 4-digit password will be needed. Secondly, a secured communication link will be ensured by an optimized Advanced Encryption Standard (AES) processor between ATM machine and the bank server. Here fingerprint image will be used as an encryption process and 4-digit password will be the symmetric key for the encryption process.

In this paper [10], some researcher discusses about how the security can be improved by using OTP and fingerprint. The process is that the actual user scans his/her ATM card in machine. When the card is scanned, the respective 12-digit RFID tag is read. Then the system passes the last 3 digits of the tag as a string and pass that as a parameter for opening the respective filename. After that the system sends a 4-pindigit in machine. If OTP is wrong, machine will show OTP is invalid. If the pin is correct, authentication comes into picture. There is also fingerprint verification system. The user can be verified by fingerprint verification. If the same user is not physically present, instead other genuine user's relative is present, he/she has to select the OTP mechanism. When he/she selects the OTP option, the system generates a random OTP and sends it to the registered sim then the real user gives

the OTP to his/her relatives. After that user can receive money.

Mithun Dutta [11] proposed that when a user enters their card into an ATM machine, GPS will automatically detect their location. Then the consumer is asked to press 4-digit pin number. If 4-digit pin number and the fingerprint match then consumer is allowed to withdraw cash. If verifying 4-digit pin number and fingerprint does not match card will be blocked and details will be sent to consumer through a message.

Christiawan [12] proposed a system that uses fingerprint and PIN system. When consumer inserts the card, he/she is then asked to input the pin. On successful pin authentication, program will then prompt for fingerprint on the sensor. After efficient authentication, the user will be taken to the key transaction menu. In the case of unsuccessful authentication, the user will be asked to repeat the process.

Syeda Prima Tasnim, a student of Brac University, Bangladesh worked on a project that used biometric recognition and a mobile application to create a dynamic link for ATM transactions. In this system, there will be a mobile app in smart phone. When a user wants to do transaction at first the user need to log into the mobile app then the app will search for the nearest ATM booth and after finding the booth user will get notification of the ATM location. After that the app will get connected with the nearest ATM by using Bluetooth then user have to submit his/her account number and the amount of transaction after that the app will ask for fingerprint from user for biometric verification, if fingerprint matches the transaction will complete and if not, then no transaction will take place [14].

Imran M.A., Mridha M.F and Nur M.K. [13] proposed a system that user don't need to carry their card all the time. Instead of biometric data, they used a specific number called BPIN and a One Time Password (OTP). The six-digit Bank Identification Number (BIN) and the four-digit Personal Identification Number (PIN) make up the BPIN. They also used an OTP, or one-time password, which is a randomly created one-time number that decreases the vulnerability of biometric knowledge. They think these are effective for those who cannot carry the card all the time.

After reviewing the model proposed in [13], we feel that there are some problems in this model. Because this model cannot fulfil the security authentication properly. Here is some point of disadvantage in this model:

- In this model card-less transaction will happen but user have to remember the BPIN always. So, if user want to save the BPIN in their phone it can be harmful because phone can be stolen or anyone can use the phone with a motive of hacking the BPIN. Because hacker do not need any card for transaction.

- As the OTP will be sent as a message in phone and it is a card-less transaction. So, anyone can steal the phone and can take the money out from ATM easily.

- This model only has two step verification. Because of this two-step verification process BPIN is quite weak so security breach may occur.

3. PROPOSED MODEL

In our designed model we have used two types of security authentication system. One is simple security authentication

and another one is strong security authentication. The entire process is diagrammatically explained in the flowchart (fig. 1) provided on the next page.

First of all, insert the card in the ATM machine. Then you need to input the BVPIN (Bank Verified) in ATM machine which is given by the bank usually. After entering BVPIN system will check whether it is verified or not. If BVPIN is verified then user can proceed for next step. When BVPIN will not verify then it will go back to the Enter BVPIN option for giving the correct BVPIN again.

After completing those steps, you have to select the security option between simple security authentication and strong security authentication.

If you select simple security authentication then you need to follow the next procedure step by step. First of all, you have to give the fingerprint in ATM machine which is registered before in the bank database at the time of account opening. After giving the fingerprint the system will check that if the fingerprint is matched or not. If the fingerprint is verified then user can do their transaction or can check other information regarding their balance or their account. And if the fingerprint is not verified then the system will show a message on the ATM screen that "Fingerprint is not verified" and the system will end the process and it will take the card out from the machine and show the Home page on the ATM screen. After that again you have to repeat the process from the starting point which is inserting the card in the ATM machine.

The second security option is strong security authentication. For strong security authentication you need to follow the processes step by step which is mentioned below:

- After selecting the strong security authentication, a question will pop out in the screen which is "Phone Number is registered for strong security purpose?", If the user's phone number is not registered before (that means if it is user's first attempt for applying strong security authentication) then the user will select no. After selecting no the system will go back to the add fingerprint part of simple security authentication. if the user's phone number is registered before that person will select yes and then a message will be visible on the ATM screen which is "Please turn on the GPS from your phone and select NEXT in the ATM for further process". After select the NEXT button you have to choose one option between fingerprint and OTP.

- If you choose fingerprint then a notification will arrive in your registered phone number to provide your fingerprint that is recorded in the bank database and after giving fingerprint the system will check if the fingerprint is verified or not. If the fingerprint is verified then user can do the transactions but if the fingerprint is not verified after two times attempt (initial value of i=1) the system will show a message that "Fingerprint is not verified" and the system will take the card out from the ATM machine.

- If you choose one-time password (OTP) then a message will be sent containing an OTP in your registered phone number. After that you have to enter the OTP in the ATM machine within 40 seconds because the OTP will only be valid for 40 seconds. Then the system will check if the OTP is verified or not. If the OTP is verified then you can

do the transaction and if the OTP is not verified then it will show a message that "Wrong OTP". Again, for new OTP user will press the Resend button and then the system will check that for how many times the resend process is applied. If it is applied for one time (initial value of j=1) then a new OTP will be sent in the registered phone number and the system will go back to the input OTP option and if it is more than one time than the process will end.

Working procedure of GPS system: The Global Navigation Satellite System (GNSS) network is used by GPS. This network is connected with the satellite and it discharge microwave signal which is transmitted to the GPS devices. It can help us to check out any information regarding location [15]. So, when you turn on the GPS from your phone it will track the location of the ATM booth from where you are doing your transaction and this location history will be saved

in your bank database so that if you need to check any location related information you can go to the respected bank and can check the location history from their stored database.

Working procedure of fingerprint system and OTP system: At this present generation everyone is using smart phone and it has an option named fingerprint sensor which is basically used for security purpose. In smart phone optical sensor is used for tracking fingerprint. There is a Light source (LED) which assists in accurately capturing your fingerprint and take a digital image with the help of CCD or CMOS and the light sensitive microchip turns the digital image into binary codes for user. If this binary code matched with the stored fingerprints code only in that time the fingerprint will be verified [16]. The OTP (one-time password) works as a random number password. Every time it generates a random number.
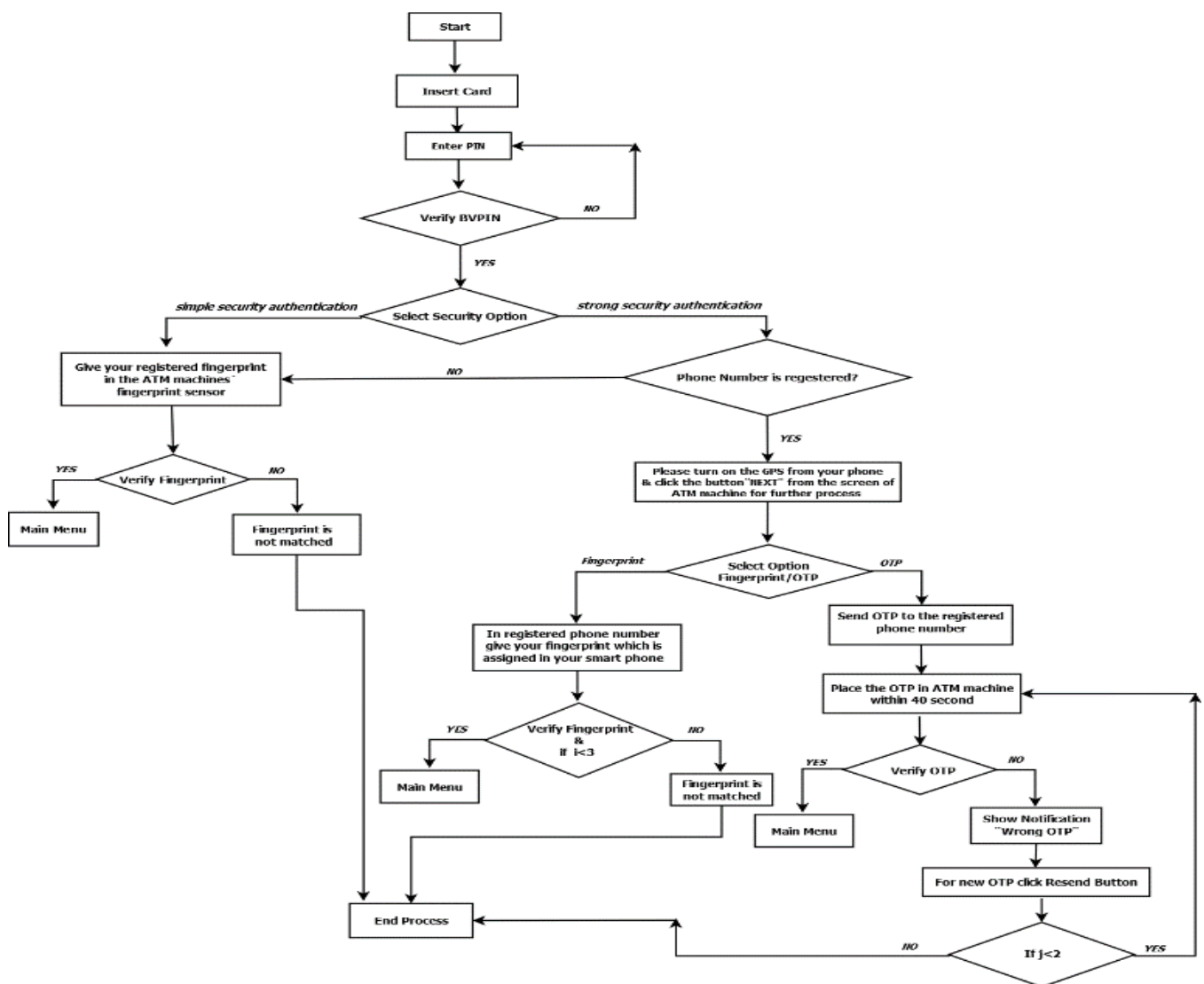

Fig 1: Flowchart of the proposed model

4. ADVANTAGE OF PROPOSED MODEL

As per our observation the model we have proposed in this paper will give much better security for ATM transaction as there is the benefit of using personal smartphone and the option of usage of either OTP or fingerprint depending on

user preference. So, if any hacker wants to hack the PIN using thermal camera or detecting the finger imprint from plastic PIN pad when user press the button from PIN pad for entering the PIN [17], hacker can do that but this will cause minimal problem because in our model there are two more remaining verification steps before doing transaction. For OTP, a time limit is given for 40 seconds and since this is one-time

password it will be difficult for the hacker to be successful because the OTP can be used only once and will be workable during a very narrow time limit. As for fingerprint option client have to give their fingerprint from their own smart phone so it will be comparatively safer to security threats than other available options. Also, the GPS process will track the location from which booth a client is doing the transaction. So even if the ATM card gets stolen the culprit can be caught red handed if they attempt to do any sort of transaction. Furthermore, as there is a benefit for giving fingerprint from smart phone so for any emergency case if user want to do their transaction by other trusted registered person that can be done as well because user will have the advantage of maintaining the security from their smart phone. Hence, this is a somewhat simplified procedure to conserve the security of transaction within few steps.

5. COMPARISON BETWEEN PREVIOUS WORK & OUR WORK

In research paper [6], Principal Component Analysis (PCA) is a software which is used for face recognition where multiple face expression images can be detected. That's why it's not only time consuming but also a high-costing process. In our work, we are using fingerprint sensor for security authentication. Since fingerprint sensor is using from years and nowadays almost every smart phone contains fingerprint sensor so there will be no extra cost and it will not be time consuming either.

In research paper [13], BPIN is used for security authentication and this BPIN is consist with ten-digits. It is a bit difficult to remember this digit. Another point is this is a card-less transaction which can hamper the security. We are using ATM card for the transaction and there will be a BVPIN (5-digit) which is the first process in our security system. As we are using ATM card so it will give a protection for transaction and as the size of BVPIN is small so it will be easier to remember.

In research paper [14], a mobile application is created through which transaction can happen and there is also a biometric system for authentication. In this app Bluetooth service is using for searching the nearest ATM booth but the range is not compatible for all devices. But in our model, there is no limitations for distance.

6. CONCLUSION

In this paper our main purpose is to upgrade the security of ATM card usage. Everybody knows that bank is a cardinal asset for a country and ATM card system is one of the vital parts of a bank. Nowadays people are using ATM card frequently but there is still a big issue for ATM users regarding ATM security. So, keeping this matter in mind we proposed a trifecta system to maintain and enrich the ATM transaction security. Since OTP will be changed from time to time and fingerprint will be given from smart phone user satisfaction regarding ATM transaction security and financial integrity of the bank will be preserved to a greater extent.

7. REFERENCES

[1] Moses Okechukwu Onyesolu and Ignatius Majesty Ezeani, "ATM Security Using Fingerprint Biometric Identifer: An Investigative Study", International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 3, No.4, 2012.

[2] B V Prasanthi, U Padma Jyothi, Sridevi Bonthu and T Vamsi Krishna, "Security Enhancement of ATM System with Fingerprint and DNA Data", International Journal of Advanced Research in Computer Science and Software Engineering (12), December - 2014, pp. 477-479.

[3] Srivatsan Sridharan, Gorthy Ravi Kiran and Sridhar Jammalamadaka, "Improvising Authenticity and Security of Automated Teller Machine Services", International Journal of Computer Science and Mobile Computing, ISSN 2320–088X, Vol. 3, Issue. 2, pg.666 – 674, February 2014.

[4] Jaydeep Shamdasani and Prof .P.N.Matte, "Atm Client Authentication System Using Biometric Identifier & Otp" , International Journal of Engineering Research and Applications, ISSN : 2248-9622, Vol. 4, Issue 4(Version 5), pp.74-78, April 2014.

[5] Krishna Nand Pandey, Md. Masoom, Supriya Kumari and Preeti Dhiman, "ATM Transaction Security Using Fingerprint/OTP", Volume 2, Issue 3, JETIR (ISSN-2349-5162), March 2015.

[6] Mohsin Karovaliya, Saifali Karedia, Sharad Oza and Dr. D. R. Kalbande, "Enhanced security for ATM machine with OTP and Facial recognition features", International Conference on Advanced Computing Technologies and Applications (ICACTA2015), 2015.

[7] Frimpong Twum, Isaac Kofi Nti and Michael Asante, "Improving Security Levels In Automatic Teller Machines (ATM) Using Multifactor Authentication", International Journal of Science and Engineering Applications Volume 5 Issue 3, 2016, ISSN-2319-7560 (Online).

[8] Mithun Dutta, Kangkhita Keam Psyche and Shamima Yasmin, "ATM Transaction Security Using Fingerprint Recognition", American Journal of Engineering Research (AJER), e-ISSN: 2320-0847 p-ISSN: 2320-0936, Volume-6, Issue-8, pp-41-45,2017.

[9] Dondo Jacqueline Akinyi Madara, Dr. George Okeyo and Dr. Michael Kimwele, "A Fingerprint & Pin Authentication to Enhance Security At The Automatic Teller Machines", International Journal of Scientific & Engineering Research, ISSN 2229-5518, Volume 8, Issue 4, April-2017.

[10] Hari Narayanan, Uttham K, I Mohammed Junaid and Mohammed Ibrahim, "Advanced ATM Multilevel Authentication Using Fingerprint Verification and OTP Validation", International Journal of Advanced Research in Computer Science (ISSN: 0976-5697), ISBN: 978-93-5311-910-2, Volume 9, Special Issue No. 3, May 2018.

[11] M. Dutta, K. K. Psyche, T. Khatun, M. A. Islam and M. A. Islam, "ATM Card Security Using Bio-Metric and Message Authentication Technology", 2018 IEEE International Conference on Computer and Communication Engineering Technology (CCET), Beijing, 2018, pp. 280-285, doi: 10.1109/CCET.2018.8542227.

[12] Christiawan, B. A. Sahar, A. F. Rahardian and E. Muchtar, "Fingershield ATM – ATM Security System using Fingerprint Authentication", 2018 International Symposium on Electronics and Smart Devices (ISESD), Bandung, 2018, pp. 1-6, doi: 10.1109/ISESD.2018.8605473.

[13] Imran, M. A., Mridha, M. F., and Nur, M. K. (2019), "OTP Based Cardless Transction using ATM", International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST), doi:10.1109/icrest.2019.8644248,2019.

[14] Syeda Prima Tasnim, "A framework of biometric recognition and personalized mobile application to establish a dynamic connection with the ATM to enable secure transaction", Department of Computer Science & Engineering, BRAC University, August 2019.

[15] "How GPS Works".University of Tasmania in conjunction with Geoscience Australia as part of the AuScope GPS in Schools Project – 2014.

[16] Tom Harries,"How Fingerprint Scanners Work". September-2002.

[17] Chester Wisniewski, "Stealing ATM PINs with thermal cameras". August-2011.