Using Fingerprint, Pycrypto, and Mobile Banking App, to withdraw cash from ATMs in Developing Countries. (A Confrontation to Eavesdropping Attack based on One-time Password (OTP))

Nachaat AbdElatif Mohamed[1], Aman Jantan[2], Abiodun Esther Omolara[3]

*[1, 3] Students Ph.D. First Year School of Computer Sciences. Universiti Sains Malaysia
Penang, Malaysia*
*[2]Second Professor School of Computer Sciences. Universiti Sains Malaysia
Penang, Malaysia*

---***---

Abstract - *Automated Teller Machines (ATM) has always been a major target for criminals. Securing ATMs remains a principal concern for the ATM manufacturers and most of the banks in the world. In the past, hunting an ATM machine involved using heavy, sophisticated tools and hardware such as explosives. However, the emergence of Digital Age changed how attacks on ATMs are perpetrated. Recent events have shown how ATMs can be robbed without even getting physical access to any hardware. While trying to address this challenge, a few methodologies and frameworks have been proposed by specialists and scientists in security. Nevertheless, some threats and vulnerabilities to ATM machines remain unsolved. In this paper, we propose how to improve the security of ATM systems using biometric fingerprint, Mobile Application, and PY crypto application. We demonstrate how to withdraw cash using this proposed system. Moreover, we increased the speed with which each transaction take place from about 30 seconds to 5 seconds. Considering that the frequency of fraud in the banking industry in developing countries keeps escalating, the methodology of this research cannot be disregarded.*

Key Words: *ATM, Pycrypto, Eavesdropping Attack, OTP, attack, IoT.*

1. INTRODUCTION

The use of Automated Teller Machines (ATM) has developed quickly in fame due to its low banks' transaction cost and clients' convenience which has made it a fundamental component of today's financial service delivery. This progress is also attributed to the convenience of transacting at anywhere or anytime, coupled with the fact that time is saved and energy reserved for other activities. Nevertheless, the ATM which is intended to serve the clients better is now turning into a serious nightmare for clients due to the number of fraud sustained in their accounts during ATM transactions. ATM crime has grown to become a worldwide issue that affects not solely customers but also bank administrators. This vexatious experience by clients is one of the challenges of deploying an ATM in the banking industry. In view of the issues experienced with ATM card fraud, banks have attempted to address this problem using encryption on the PIN on the card to deter criminal and hackers efforts at siphoning peoples money. Even so, hackers still find sophisticated tools, tactics, and techniques to evade this security and acquire peoples money.

Recent occurence of the Carbanak Cyber crime is a clear indication that hackers have gone haywire with their sophisticated techniques in siphoning cash [16]. The Carbanak attackers used remote commands to instruct ATMs to dispense cash without any interaction with the ATM itself. Mules were then used to collect the cash from the ATM.

This research proposes an improved way of securing ATM machine transactions and show how to increase the speed at which transactions occur. The two major contributions of this research are:

- We show how to withdraw cash by fingerprint with mobile application and save the user time
- Secondly, we pictoriacally demonstrate how to increase the security of the bank, customer, ATM Machine and improve the one-time password pin used for transactions.

In this Paper, we present a structure which uses a software, Pycrypto, OTP, and fingerprint to allow a user to withdraw cash only in 5 seconds. Knowing that to get the cash by the traditional way takes at least 30 seconds or more, [3] this is surely an improvement on a conventional system.

If the proposed system is applied correctly in developing, and developed countries, it can save massive amount from being siphoned. The objectives of World Bank`s by 2020 is to foster financial inclusion, but the traditional access channels, like ATMs Machine, are very limited in developing countries. For instance, a country like Egypt, [2] is limited in this area as nearly half adult urban population in Egypt does not have credit cards, completely unbanked. Studies showed that only 17% own a payment card and that 97% of Egyptian employees. Receive their salaries in cash. This statistic was taking from urban areas. What about the countryside? [7]. The question is, what will happen if these huge percentage of people requested to be banking? Egypt is one of the fastest growing Visa market in the Middle East and North Africa (MENA) region. Egypt's growth in card numbers far exceeds the 30% average regional increase for MENA. Moreover, the results show an increase in the number of visa card acceptance in Egypt by 6% to reach a total of 27,663 locations, including 23,910 merchant outlets (up 4% year-on-year) and 1,912 ATMs (up 46% year-on-year), [7]. Most researchers have tried to improve the functionality of ATMs [3]. On the other hand, our work will reflect on ECC (Elliptic-curve cryptography) which leverage on secure OTP, to avoid eavesdropping, social engineering, and brute force attacks at ECC, [1]. As we know every single electronic device connected to the internet is at risk of penetration. In retrospect, we propose an alternative approach for fast and secure operations during ATM transactions. Figure 1 presents a taxonomy of the ATM setting. The system consists of an integration of work at different levels; user, application, database, and security. Moreover, the system will be integrated with IoT. In conclusion, a great leap in saving customer time, effort, and an improvement in the security will be achieved.

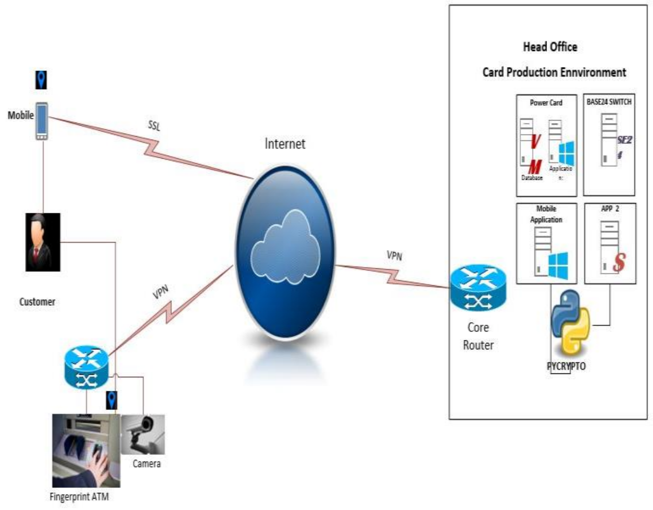

Fig -1 our Project design.

2. State-of-the-Art

Nowadays most transactions are carried out through mobile devices because it saves time and effort, but unfortunately to withdraw cash remains a dilemma for majority of the people in the world. You can withdraw cash from anywhere, but still you must wait in the queue in front of ATM. In some cases, it gets more annoying because you have to select and filter through unwanted options like language, amount, and print options. Recent studies have shown how money can be withdrawn faster using QR-code via the mobile banking Application [3]. Relatively, there are banking manual service and E-Banking services, though E-Banking services are deemed better, but do not provide satisfactory quality, [4]. There are several vulnerability when using card on ATM. When a customer stands behind ATM machine, another one can watch his password/passcode, and this code can be exploited easily by hackers to recover the customers money. To overcome this problem, several suggestions has been made such as using cognitive systems like Face recognition system, face expression, DNA, gaits, fingerprint identification, et cetera [5]. Also, we can use micro bank service to automate withdrawal and deposit money and connect it with bank server through (RASPBERRY-PI). The customer can then call customer care division, and inform where he want to withdraw/deposit the money. The bank then chooses a micro bank unit, and send query message. The micro-unit will reply acknowledgment, then bank server will send OTP to customer, micromachine will receive the same OTP, the microbank system always connected with central banking server using GSM communication, [6].

3. Project Proposal

The motivation of withdrawing money by mobile banking Application to save the customer time, effort, and improve all of the security elements during this operation, of course, some people converse about this project. I will take up the subject creatively, and try to cover all aspects, beginning with the customer request withdraw service until he receives the amount from ATM. This Project based on Encryption/Decryption PY Crypto. "The various IM clients can be classified into three types according to their provided encryption protocols: no encryption, client-to-server encryption, and client-to-client or end-to-end encryption (E2EE)", [8]. Frist of all, Bank must request from all customers to update them data, to allow the bank registering customer fingerprints in the bank database, then, customer will demand a withdrawal amount through his mobile banking application, in related request customer location will be sent to the bank, bank will select the ATMs that located in the same area, and then determine the number of people front of each machine through cameras installed (this operation will be done automatically), the Application must suggest the best solutions in terms of distance from the client and the smallest number of people, then binds the OTP with customer fingerprint which will be incepted through PYcrypto, customer will receive the message ask him go to the nearest ATM which be mentioned in the message with request button in same message ask him (when you front of ATM, confirm that), after the customer arrived at ATM will press the button in the massage the bank will reply with OTP (but the good news is, customer will not use at all OTP), only he will use his fingerprint to take the amount directly, also w have another good news at this point, if any hacker eavesdropped the OTP he cannot do anything by this number, because this number only to inform the customer that your amount is ready. Imagine the worst case, any hacker succeeded to eavesdrop the massage which includes the location of ATM, the third good news is, he cannot receive any cash, because the money only receives by customer fingerprint.

4. Terms and background

Pycrypto is Python toolkit, with a selection of implementations of cryptographic algorithms including a random number generator. It is time-saving and increases the Security, [9]. Other subpackages of the Pycrypto includes; Crypto.Cipher, Crypto.Hash, Crypto.Protocol, Crypto.PublicKey, Crypto.Signature, and Crypto.Util.

Eavesdropping Attack is the unauthorized interception of private communications between two parties. This could include messages, phone call, video or fax transmission. It looks like someone standing under the eaves of a house and listening to conversation been made. The conversation between tow device containing many nods, if a hacker compromises only one node, he can access the IP packets flowing through that node, many tools can allow striker to save a conversation, [10]. Encryption is one of the best Countermeasures to face eavesdropping attack, [10].

OTP (One Time Password) is a password that is valid for only one session at the digital system service, it is a secure and fixed password which is not vulnerable to replay attacks. To receive an OTP, a customer is prompted to the enter his username/email address or registration number or both (based on application policy). If he supplies correct credentials, then his account will be enabled to receive the OTP. Once the user is authenticated, he gets the One-Time password, [11].

IoT (Internet of Things) is the network of physical devices, vehicles, mobile, tablets, laptop, home appliances and other items embedded with electronics, software, sensors, actuators, and connectivity which allows these objects to communicate and exchange data. Recent research predicted that by the year 2020, about fifty (50) billion of such devices are expected to be deployed [12].

ECC (Elliptic Curve Cryptography) is an algorithm that allows key sharing, information transferring and mutual authentication between clients or users and the central server in a secure manner, [13].

5. Challenges

In our research, we faced a challenge as banks refused to cooperate with us due to, we need cooperation with some banks to study the real situation, cost, Legislation to obtain customer fingerprint, devices.

6. Research goal

The most significant two aims of this research are, saving the customer time while carrying out transaction, and an increase in the security level which currently is not supported in traditional ATM setting. Usually, a customer needs about thirty (30) seconds or more to get his cash from ATMs, but the method proposed in this paper will allow the same transaction for a shorter period of five (5) seconds. On the other hand, we will improve the security, in protecting private communication between customers, mobile app, and ATMs. We will make a relation between customer fingerprint and OTP (one-time password), then generate a secured number based on customer fingerprint, he will use it only to withdraw his money in 5 second. This feature will add value to the bank's services, the bank can market it to attract the customer.

7. Critical scenario

1- Use fingerprint to withdraw cash.
2- Use D.QR-code to withdraw cash
3- Use Barcode to withdraw cash
4- Use finger eye to withdraw cash.

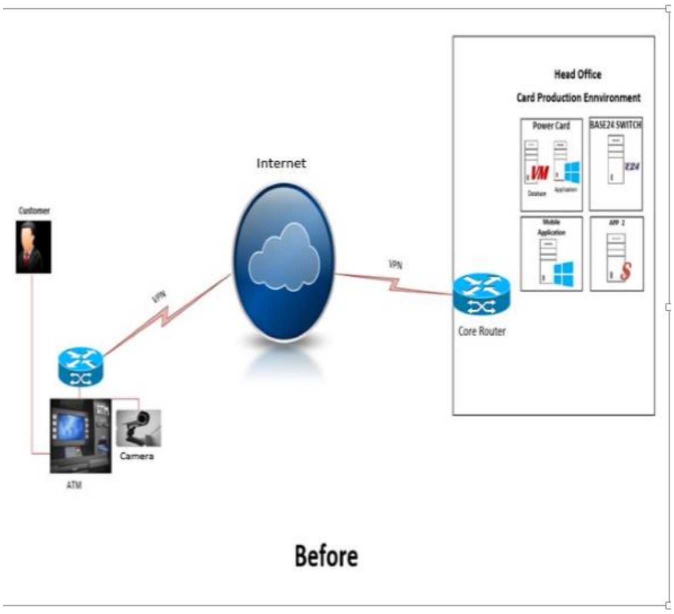

Fig -2 Before Implement our project.

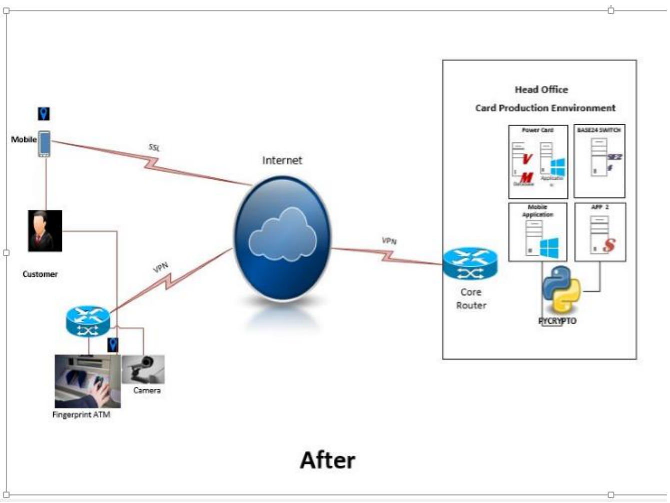

Fig -3 after Implement our new contribution.

8. Expected results

This research aims to design, implement, and evaluate a new concept to withdraw money through Pycrypto, fingerprint, and mobile banking Application. The proposed system guarantees a high efficiency to save a customer's time and improve the security to protect a customer's privacy, and credential data. In the case of ATM security, the proposed system enhances the ATMs security and more privacy protection for the customer during any transactional operation. In addition, we improved the current OTP (one-time password) by connecting it with fingerprint number which will be secured by PY Crypto. Then we will use PY to encrypt and decrypt the sensitive numbers in this project. There is no time wasted in carrying out a transaction as in the traditional way, and no need to stand in the queue to get cash. This research is highly profitable for industries especially if implemented in specific country's (developing countries). Finally, we can customize the project as appropriate for each country, and the system can be integrated with the Internet of things (IoT).

9. Conclusion

In this paper, we have explored a critical scenario, D.QR-code, Barcode, finger eye, and fingerprint to withdraw cash. We focused on how to be using py crypto, a fingerprint to get your cash, and described the Encryption is one of the best Countermeasures to face eavesdropping attack, we used it with parametric to give maximum protection through withdraw cash operation.

ACKNOWLEGMENT

The authors gratefully acknowledge the anonymous reviewers for their constructive comments, ideas and suggestions.

REFERENCE

[1] Yadav, Deepak, et al. "Intensify the security of one-time password using elliptic curve cryptography with fingerprint for e-commerce application." International Journal of Engineering Science 5480 (2017).

[2] Cámara, Noelia, David Tuesta, and Pablo Urbiola. Extending access to the formal financial system: the banking correspondent business model. No. 1510. 2015.

[3] Hajare, Uday, et al. "Efficient Cash Withdrawal from ATM machine using Mobile Banking." (2018).

[4] Rahman, Mahbub, et al. "Problems and prospects of electronic banking in Bangladesh: A case study on Dutch-Bangla Bank Limited." American Journal of Operations Management and Information Systems 2.1 (2017): 42-53.

[5] Risodkar, Y. R., et al. "ATM Authentication with Enhance Security Using GSM." Journal of Science and Technology (JST) 2.5 (2017): 01-05.

[6] Kumar, V. Naveen. "Research Scholar "Advanced Handheld Electronic banking System using Raspberry pi." Advanced Research Journals of Science and Technology (ARJST) 4 (2017): 276-279.

[7] El-Gawady, Zeinab Mohamed. "Relationship between E-money and Monetary Policy in Egypt." (2018).

[8] Lee, Jeeun, et al. "Security Analysis of End-to-End Encryption in Telegram." SCIS 2017 (2017).

[9] Butschek, Caroline. Using Autocorrelations to Detect Potential Side-Channels. Diss.

[10] Velianitis, Georgios, et al. "Comparison of VoIP and TETRA regarding security in a safety critical environment." Journal of Computers 13.3 (2018): 279-287.

[11] JIni, Mrs A. Jackulin Sam, et al. "TENABLE ONLINE ISSUE OF BIRTH CERTIFICATE FOR REGIME CONGLOMERATE." (2018).

[12] Sheth, Amit, Biplav Srivastava, and Florian Michahelles. "IoT-Enhanced Human Experience." IEEE Internet Computing 1 (2018): 4-7.

[13] Jegadeesan, S., et al. "ECC based Algorithms for Secure Water Quality Monitoring System Using Wireless Sensor Networks." (2018).

[14] Pal, Joyojeet, et al. "Digital payment and its discontents: Street shops and the Indian government's push for cashless transactions." (2018).

[15] Oye, N. D., and Jemimah Nathaniel. "Fraud Detection and Control System in Bank Using Finger Print Simulation." (2018).

[16] Johnson, Ariana L. "Cybersecurity for financial institutions: The integral role of information sharing in cyber attack mitigation." NC Banking Inst. 20 (2016): 277.