ATM Security with Hashed Biometrics as Multifactor Authentication - Research Proposal

Anojithan Pakkiyarajah

Department of Information Technology Specialization in Cyber Security
Sri Lanka Institute of Information Technology (SLIIT)
New Kandy Rd, Malabe 10115, Sri Lanka.

ano.tech2@gmail.com
Virtusa (Pvt) Ltd,
752, Dr Danister De Silva Mawatha, Colombo 00900, Sri Lanka

I. INTRODUCTION

Technology advancement never miss to disappoint the security. So, it's been a must to have a perfect security that aligns the architecture of the imposed system. Today, banks suffer the most uttermost crisis of security, even though it has been equipped with high standard security implementations, still the end devices fail to do their job right. There are number of ATM theft happing around the world. The attackers / unauthorized individual make use of the stolen card or skimmers to get it done.

Considering the above, introducing biometric scanners and OTP as a means of multifactor authentication for higher transaction can ensure the second level of security in the ATM transactions.

II. PROBLEM STATEMENT

Due to the technological advancement in the field of banking, electronic cards, online transactions and e banking has becomes an inevitable resources, where automated Teller machine plays (ATM) plays an important role. Unfortunately in the other hand, ATM theft has exposed to exponential growth in past decade [1]. The main reason for this could be, the person with the electronic card and know the PIN can withdraw money without any obstruction. There is no strict barriers or authentication between the end device such as ATM and the individual interacting with. Therefore stolen card can be used to withdraw money with 4 digit / 6 digit PIN code. There are few ways how the PIN can be exposed to unauthorized induvial. The most common way of exposing the PIN can be skimming attacks. European ATM security team states that there are rise in ATM skimming. They also stated that there are 24% of increase in theft during the mid of 2009 [1].

Abhilesh S. Jadhao and Shital B. Kumbhalkar stated that ATM transfer while transaction might be unsecure as it has the probability of smart or electronic cards get cloned with replica ATM cards with the aid of magnetic stripes, which are attached to the ATM machine's card slots. The reader would be able to capture the data available on the victim's card and store the particular data for later usage. The practice of Replay attacks [2].

III. OBJECTIVE

The long term goal of this research is to provide adequate security measures for the stolen card ATM transactions forgeries with the use of biometric devices and cryptographic technique. The secondary objective of this current study is to provide comprehensive literature review of well-known authors on how mitigating the flaws and the constraints on applying it to the real world. This will bring the trust between the users and the financial sectors (Banks) even though their electronic cards stolen along with the PIN, the forgery cannot be done. I strongly believe that once this security measures applied on today's ATM architecture / Framework the probability of theft related to stolen card will be minimized.

IV. THEORETICAL FRAMEWORK

In the means of providing another level of security which can minimize stolen card forgery related to ATM transactions, there are two main things involved. Which are Secondary authentication and proper use of sensitive data.

1. Secondary authentication

Secondary authentications in other words multi factor authentication, which means along with the traditional PIN, having another step of verification procedure to ensure the authorized individual accessing the transaction. Involving biometric scanners or OTP can be feasible. Abhilesh S. Jadhao and Shital B. Kumbhalkar stated that it's possible to have OTP with PIN to strengthen the security in

ATM transactions [2]. Selvaraju N and Sekar G proposed a crypto biometric authentication scheme for ATM transactions. They were discussing on giving an opportunity to read the finger print of the authorized personal before letting the transaction proceeds.

2. Proper use of sensitive data

Even though the ATM is secured with Secondary authentication technologies, the PIN, Biometric readings and the OTP cross checking has to be done or retrieved in a very secure way. In the other hand, if the sensitive data losses to unauthorized party there are possibilities of replay attacks. Z. Wu, S. Gao, E. S. Cling and H. Li clearly explains the ways how replay attacks taking place in modern networking [3]. So it's been a must to secure the sensitive data from accessing by outsiders than having more authentication techniques.

V. RESEARCH DESIGN

The primary method for this study are literature review and conceptual modeling. By analyzing well written literature the flaws in the concept has been identified, which was; there are no secondary authentication mode in current ATM transaction procedure and if that to be implemented the proper storage and retrieval mechanisms also need to be implemented.

Here I would like to propose the methodologies in two main steps, which are the Data collection at the ATM end point and the Verification at ATM. Image.01, below shows the flowchart which describes the places where the fingerprint scanning needed to be implemented to the ATM transaction.

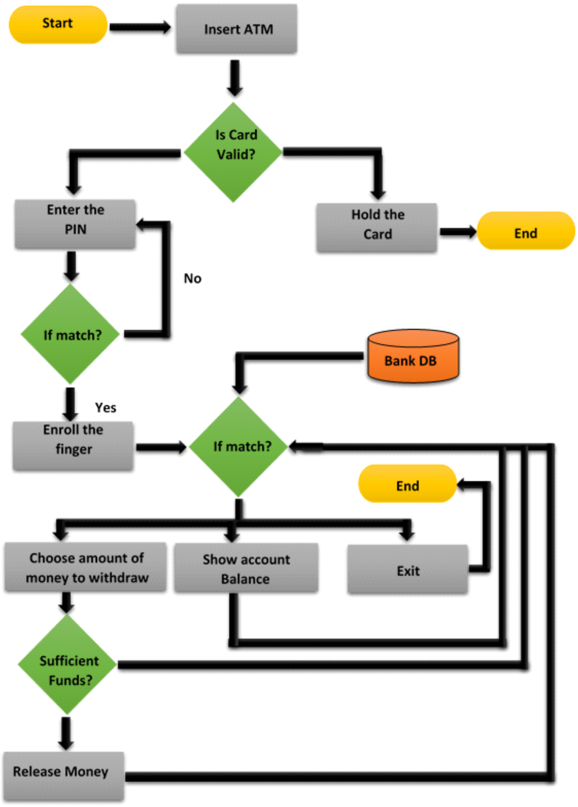


Image 01: Biometric ATM flowchart

Once just after the PIN verification, I suggest to have the enrollment of the fingerprint scanning for further authentication. There are two reasons to have biometric scanning just after the PIN is to verify whether the owner has inserted the electronic card, and that verification has to be done after the PIN matches the Card only.

Researchers Sergey Tulyakov, Faisal Farooq and Venu Govindaraju has done an excellent research and figured out key methodologies in hashing biometrics. They proposed a way to perform hash function for finger print minutiae. They also have proposed on how to create hashed biometric data for each instance [4]. They were saying encrypting biometric data and decrypting it back when needed can be overhead, and the storage of biometric data in central database seems to be unprotected. The reason for this is, when the central database is compromised by an attacker all the stored biometric data will be lost. Hence they restated the importance of storing the hashed biometric data. Still producing the exact same hash for same fingerprint is not practical, because the registered fingerprint depends on the way it was recorded. It can be the degree of the finger placed or where the finger is placed and so on. Even a very small difference can bring a huge difference in the produced hash. To overcome the problem which is mentioned above, they proposed matching hash using localized set of minutiae, and global matching of two fingerprints as a matching with similar transformation parameters. In addition they have come up with an algorithm to resolve this issue. They have discussed this under the heading “Security of Proposed Algorithm”.

The next function to be done is, Hashing function with salting. Pritesh N. Patel, Jigisha K. Patel and Praesh V. Virparia states that, in the technique of password protection with salted hashing, salt refers to a random string of data which is used to modify a password hash. This is done to prevent the identification of identical password, as the salt value added password can be completely different and un-identical hash value [4]. Simply if two or more users use the same password, the addition of salt value gives hash values which are totally different. Which is protecting rainbow table attacks. Those days the Random numbers were generated by Pseudo Random Number Generators (PRNG) and now the random numbers are generated by cryptographically secure Pseudo Random Number Generators (CSPRNG) [4].

There are five main steps involved in generating the salt hash value. And they are respectively,

- Getting the data need to be hashed.
- Generate salt using trusted random methods / functions.
- Append salt to the data to be hashed.
- Generate salted hash using appropriate Hash function (MD5 \ SHA256)
- Store salt value, salted hash value, User’s / function’s ID, etc. in the database.

With the above mentioned technique the salted hash value for the fingerprint can be obtained. At the ATM, the machine follows from step 1 to step 4, to generate the salted hash value for the fingerprint. For the validation purposes, the ATM terminal collects the salt value stored in the Bank database and follow the first four steps and then calculate the salted hash value. If the both hashed values are identical then the fingerprint seems to be authorized. Image 02 below, describes on how the validation is taking place in a simple flowchart.

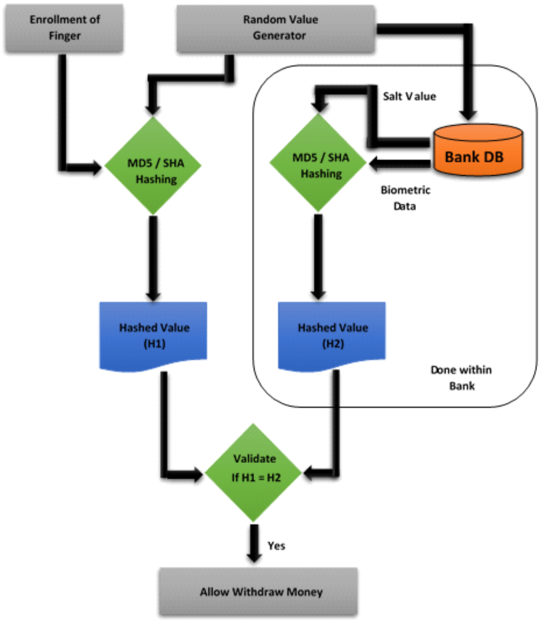


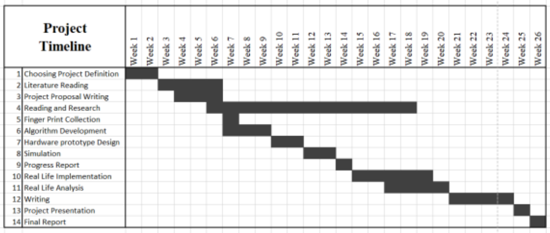
Image 02: Biometric Hashing and verification flowchart

VI. RESOURCE REQUIREMENT

To start this research a set of data need to be collected, the most important one is the biometric scan of random individual which is simply finger prints. Also this finger print scans need to be collected in various times, various degrees and in various pressure. Apart from finger print details need to re-program the algorithm that fits the requirement. The algorithm needs to be modified in a way which is able to detect the same biometric reading in different instances. In hardware perspective there's a need for model ATM infrastructure to perform the testing. Which can be built using Raspberry Pi.

VII. PLANNED TIMELINE OF RESEARCH STUDY

I have planned to finish this project within the time period of six months, approximately 26 weeks. So far the project reached its' 10th week. Hopefully end of June a final report will be submitted for administrative inspection. Table 01 shows the timeline in graphical format.



Project Timeline		Week 1	Week 2	Week 3	Week 4	Week 5	Week 6	Week 7	Week 8	Week 9	Week 10	Week 11	Week 12	Week 13	Week 14	Week 15	Week 16	Week 17	Week 18	Week 19	Week 20	Week 21	Week 22	Week 23	Week 24	Week 25	Week 26
1	Choosing Project Definition	■	■																								
2	Literature Reading			■	■	■	■																				
3	Project Proposal Writing				■	■	■																				
4	Reading and Research						■	■	■	■	■	■	■	■	■	■	■	■	■								
5	Finger Print Collection							■																			
6	Algorithm Development							■	■	■																	
7	Hardware prototype Design										■	■															
8	Simulation												■	■													
9	Progress Report														■												
10	Real Life Implementation															■	■	■	■	■							
11	Real Life Analysis																	■	■	■	■						
12	Writing																					■	■	■	■		
13	Project Presentation																									■	
14	Final Report																										■

Table 01: Planned timeline of research study

REFERENCES

[1]Twum, Frimpong & Nti, Isaac kofi & Asante, Michael. (2016). Improving Security Levels In Automatic Teller Machines (ATM) Using Multifactor Authentication. International Journal of Science and Engineering Applications. 5. 126-134. 10.7753/IJSEA0503.1003.

[2]Anca D. Jurcut, Tom Coffey, and Reiner Dojen, “On the Prevention and detection of Replay attacks Using a Logic-Based Verification Tool”, Department of Electronic & Computer Engineering.

[3]Z. Wu, S. Gao, E. S. Cling and H. Li, "A study on replay attack and anti-spoofing for text-dependent speaker verification," Signal and Information Processing Association Annual Summit and Conference (APSIPA), 2014 Asia-Pacific, Siem Reap, 2014, pp. 1-5.

[4]P. Patel, J. Patel and P. Virparia, "A Cryptography Application using Salt Hash Technique", International Journal of Application or Innovation in Engineering & Management (IJAIEM), vol. 2, no. 6, 2013.