Intelligent ATM Securing System

Rajneesh Tanwar*, Pooja Pant** and M. Papoutsidakis***

ABSTRACT

In this modern world, all citizens having their account in any of the banks and all are getting salaries or saving their money in their bank accounts. When need of money occurs, simply get transacted from ATM machines. ATM uses password security set by owner but still many crimes are happening in which catching robber is not possible as ATM machine is not have any intelligence of detecting whether the transaction is done in some pressure or not. Many techniques are present to handle the condition of ATM card lost but still no solution of getting the card owner situation during transaction of money. To handle such type of crimes, bank database will store all family members eye iris scan and then the first authentication of card holder by PIN and second authentication will be eye iris of card holder. Camera mounted over machine will first scan eye iris to authenticate and after authentication it will scan the movement of eye iris of ATM user. If user eye iris movement is static then ATM machine will carry on the further steps for transaction of money or else work. But if scanned eye iris shows any movement and not static then it will allow for same procedure but machine at end will display zero money in bank account or card service is disabled. The implementation of this intelligence will decrease the criminal cases in certain situation.

Keywords: ATM machine, ATM card, Transaction, eye IRIS

1. INTRODUCTION

The antiquated and customary society did not have any money related instruments, thus the whole trade of products and stock was overseen by the "bargain framework" [1]. The present day society however began utilizing financial instruments as a unit of trade which now supplanted the bargain framework. In this way, cash in different divisions was currently utilized as the sole buying power as against the deal framework. The contemporary time has supplanted these customary fiscal instruments from a paper and metal based coin to "plastic cash" as Visas, platinum cards, and so forth [2]. This has brought about the expanding utilization of Automated Teller Machine (ATM) everywhere throughout the world.

ATMs are electronic saving money machines situated in better places and the clients can make essential exchanges without the assistance of bank staffs. With the assistance of ATM the client can play out a few keeping money exercises like cash exchange, money withdrawal, charge card installment, paying different home use charges like power and telephone charge. [3] It is a more helpful for clients to get to their ledgers and to lead monetary exchanges. The record holder will be given the ATM card and private PIN (Personal Identification Number) or secret key. Stick number or secret word is a critical perspective in ATM framework, which is usually used to secure and ensure money related data of clients. Stick number should be recollected by the card proprietor and it ought not be imparted to others to counteract unapproved get to [4]. Wrongdoing which is occurring in ATM turned into a difficult issue that influences clients as well as bank administrators. Security is a significant issue in ATM framework. ATM trick includes criminals putting a thin, clear, unbending plastic sleeve into the ATM card opening. By doing this way, when you enter your card, the machine can't read the strip, so it will be continue asking you to re-enter your PIN number [5]. The ATM machine has card Reader and keys as info gadgets and show screen, money container, receipt printer,

---

* Department of Information Technology, Amity University, Noida, India, *Email: rajneeshtanwar15@gmail.com*

** Department of Computer Science, Amity University, Noida, India, *Email: ashima81k@gmail.com*

*** Automation Engineering, Piraeus University of Applied Sciences, Greece, *Email: mipapou@teipir.gr*

speaker as yield gadgets. ATMs are associating with a host processor, which is a typical door through which different ATM systems get to be accessible to clients. Different banks, free administration suppliers possessed this host processor.

2.   CURRENT SCENARIO

The expansion of robotized teller machine (ATM) fakes has incited the improvement of new confirmation systems to defeat security issues of individual distinguishing proof numbers (PIN). These verification components are generally evaluated in view of speed, security, and update capacity in correlation with conventional PIN section frameworks [6]. The biometric confirmation strategy is by all accounts the most prevalent developing option component as against PIN-based ATM verification. This validation strategy however is imperfect. Fingerprints, for instance, are special yet they are not privileged insights. We abandon them wherever with all that we touch, subsequently, they can without much of a stretch be fashioned with a film [7]. The fingerprints on a man can get harmed furthermore; it changes with age [8]. Notwithstanding this, another genuine blemish with the fingerprints is that the robbery of a man's biometric prompts some major issues as reenrolment is unrealistic not at all like the resetting or changing of PIN. The current ATM framework verifies exchanges by means of the card and PIN-based framework. From that point, it gifts access to bank clients to a few administrations, for example, money withdrawal and stores, record to record exchanges, adjust enquiry, best up buys and service charges installment. The ATM framework thinks about the PIN entered against the put away approval PIN for each ATM clients. In the event that there is a match, the framework verifies the client and stipends access to every one of the administrations accessible by means of the ATM. In the event that there is a befuddle then again, the client validation prepare comes up short and the client is given two more chances to enter a right PIN. In the event that an inaccurate PIN is entered for the third time, the card gets blocked and held by the ATM. A case of money withdrawal on the current ATM framework is delineated in the move outline in Figure. 1. Section of a right PIN is satisfactory to verify a client to the bank framework and from that point allow access to the framework for withdrawal as portrayed in Figure 1 .The current framework additionally holds ATM cards after passage on a wrong PIN thrice in this manner taking out further endeavors to increase unapproved get to.

3.   PROPOSED METHODOLOGY

The proposed framework is containing stepwise authentication of the ATM user to know the situation or case in which transaction is taking place. ATM authentication through ATM pin is a static process which can't be able to behave in a intelligent way but in proposed methodology one more authentication is introduced which will behave in a smarter way with the help of the ATM user.

Proposed methodology will act or introduced after the first authentication through ATM pin or password. After entering ATM pin, all machines will carry camera embedded inside them which is not easy detectable by user and that camera will note and scan the eye iris of ATM user after entering the correct ATM pin. During the transaction process if ATM machine find that iris is not matching then transaction will get cancelled automatically by showing authentication problem. In eye iris database, it will firstly store all family members eye iris for matching and if the match is not get overlapped with any of five then the authentication problem will arise during transaction. This will work as a second authentication process for increasing safety over the ATM machine.

Secondly, the intelligence that will work behind to know or catch ATM user situation, the movement of iris will also get traced by same embedded camera and that camera will contains a property that, if the ATM user's iris movement is more then it will sense or treat that condition as bad situation of ATM user and will act smartly, it will allow the machine to follow the proper steps of transaction but at the end it will show message of insufficient balance or server problem error. So in case of money lending over the point of gun
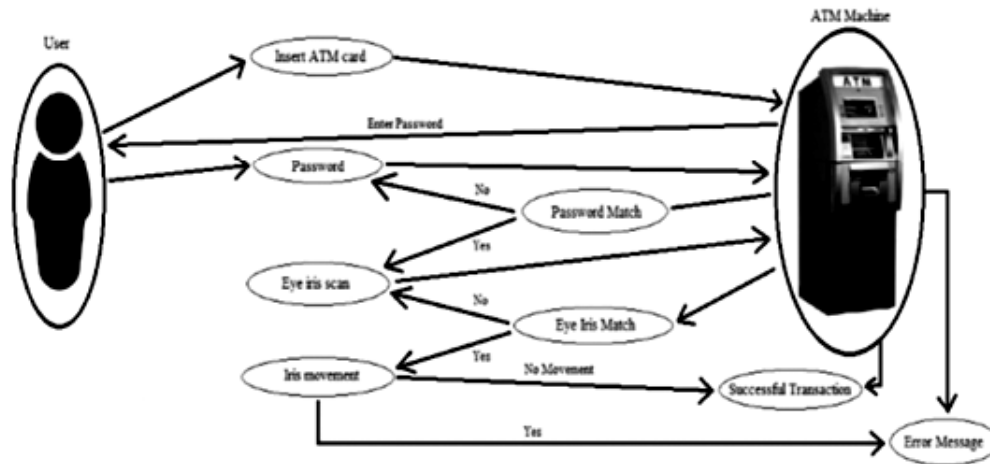
Figure 1: Flow of Proposed System

will probably get failed and user is able to save money but if ATM camera is not able to track any movement i.e. if there is no movement of eye iris then the machine will lend money to ATM user. ATM user is playing a primary role as the movement of iris is totally dependent on the user and will secondly caught by ATM camera then after intelligence part of ATM machine will process.

Fig 1 above describes the flow of how ATM machine will act smartly to achieve more security over the money of user. Up to password verification, the system will run in the same current flowing ATM machine process and after the verification of password, another new verification will also be done that is user eye iris scan and matching output with stored information in database. If not matched then it will again scan up to three times and after maximum trial the machine will automatically end up the process. If the eye iris got matched, then movement of eyes will be traced while transaction process is running in parallel. If there is lot of movement will be traced by iris scanner then Error Message will get displayed over the screen of ATM machine after whole normal process and if movement is static then transaction will get successful and money will be landed to the user.

4. CONCLUSION

With the implementation of proposed methodology, money landing over the gun point or in any criminal situation will become safer with compared to current scenario as proposed methodology contain the double verification of user which should be matched with the details of ATM owner saved in database. In second verification, eyes iris matching will act as one of the best verification of ATM user and even after that to determine the situation of user, intelligence of tracing eye iris movement will also there which build whole system to process in smart way. So the system will increase its security by changing or updating the process of transaction and if the iris movement is more than the process of transaction will flow in parallel and will drop message so that user will not able to get the smartness of process.

REFERENCES

[1] Jimoh, R.G. and Babatunde, A. N., Enhanced Automated Teller Machine using Short Message Service authentication verification. World Academy of Science, Engineering and Technology. International Journal of Computer, Information Science and Engineering 2014.

[2] Muhammad-Bello, Alhassan , Ganiyu "An Enhanced ATM Security System using SecondLevel Authentication", International Journal of Computer Application, 2015.

[3] Kande Archana and Dr. A.Govardhan "Enhance the Security in the ATM System with Multimodal Biometrics and Two-Tier Security" , International Journal of advanced research in computer science and software engineering, 2013

[4]   S.S.Das and Debbarma "Designing a Biometric Stradegy fingerprint Measure for enhancing ATM Security in Indian e-banking System",International Journal of Information and Communication Technology Research,volume.1,2011.

[5]   Jain A.K, Ross A. and Prabhakar S. IEEE Transactions on Circuits and Systems for Video Technology, 2009.

[6]   De Luca, A., Langheinrich, M. & Hussmann, H. (2010). Towards Understanding ATM Security – A Field Study of Real World ATM Use.

[7]   Kyle, C., Biometrics: An In Depth Examination. SANS Institute Information Security Reading Room. SANS Institute 2004.

[8]   Liu, N. Y., Bio Privacy: Privacy Regulations and the Challenge of Biometrics. Taylor & Francis 2013.