IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.115165

Security Solution of The Atm and Banking System

Ashwini Pyarelal Bambode[1], Lowlesh Nandkishor Yadav[2], Vijay M. Rakhade[3]

Student, Computer Science & Engineering, Shri Sai College of Engineering & Technology, Bhadrawati, India[1]

HOD, Computer Science & Engineering, Shri Sai College of Engineering & Technology, Bhadrawati, India[2]

Asst.Prof, Computer Science & Engineering, Shri Sai College of Engineering & Technology, Bhadrawati, India[3]

Abstract: As today the growth of the electronic devices are resulting in the very high demand because the things get faster because of the electronic devices we can see as for withdrawing the money one has to go the bank and stand in a Queue for money when the numbers come after two three hours then they are browning money from the bank so as today there is large number of demand of the electronic device which Automated Teller Machine (ATM) it is machine in which one can take the money immediately from the ATM whenever they want as this system works online we know that in the online system there must be security and most of them try to do fraud also in the ATM ass while in the transaction the user already gets the password and card for withdraw his own money, although this security aspect are there than also the fraud happens it has become the biggest issue for the user in order to gain trust and confident over the ATM's, purpose of this paper is to examine the different types of Automated Teller Machine, Security which has been improved for all the user who are using the ATM for transaction, This paper assumes the frame security of the ATM transaction.

Keywords: ATM, Authentication, Integrity, Security

I. INTRODUCTION

The development of the banking technology has changed for managing the user account for exchange of the money which will be quick mode, adaptable and will be the practical model, Banking technology has diminished physical communication with the staff of banks for managing the account through exchange of the Automated Teller Machine The ATM technology has extended all over the world due to this the bank staff and the customer gets relaxed because as in the bank there one has to do the paper work for transaction and stand in a Queue with the ATM system the customer can withdraw the money, balance of the account, details about last transaction, and also other online transaction like paying electric bill. The ATM is a computerized account managing, Despite all the only security of the account is that the individual has their own ID and pin for different accounts ATM also exchange the different kinds of the securities and fundamentals such as , the security of the ATM, Security of user card with the help of the ATM cheats the new confirmation system have been produced, but in the present the business layered security with end goal to give the greater security to the ATM. This security measure incorporates the security pf the Machine, transaction security, validation of the client security, and also the client security. For holding the current clients and gain the trust on the ATM the framework of the automated banking system should create distinctive refined system that will shield from the illegal accessing over the clients accounts and also furthermore self security of the client account This paper is arranged in the four section firstly providing the background research for the multiphase security , work related to the security of the Automated Teller Machine, providing the new security system, and analysing the system.

II. BACKGROUND RESEARCH

Although the crime are happening rapidly day by the in physical manner as well as the online manner, without the knowledge of the owner the ATM has twisted a general issue that influence the user as well as the financial institutions, bank services that make them questionable during the transaction of the money by the portable or a phone system. The attack of the ATM are the distinctive sort the ATM itself with the end goal has access money safe inside , robbery of the ATM card, delicate data or controlling the ATM and one of the most noticeable is harming the client life of client itself, The strategies of the client verification include the ATM card with the appropriate ID number and also the pin or the secret password can be directly obtained by the covered perceptions. At the time when the ATM is lost , or it has been stolen than the unauthorized client can without much stretch figure the pin in light of the fact that even can after controlling a few clients will be utilizing the pin as there birthday, or the telephone number, or the saving number which the government manages. A t the end of the goal the current client get a trust and confident and can get a new client , financial organizations should fuse safety system to defeat from the fraudulent clients. As the extortion moves in the different ways and also over the channel from web to the ATM system by taking the client ATM card from the

 This work is licensed under a Creative Commons Attribution 4.0 International License

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.115165

authorized client , it has been very important to see the security from the multiphase , the multiphase include the Physical security, ATM card security, Network security, and also the user security.

III. RELATED WORK

Shaikh and Rabaiotti (2010) examined the united kingdom identify card by examining they discovered that there is an exchange between security and adaptability in the biometric based framework , where as Amurthy and Reddy (2012) they build a unique embedded framework and finger print system in which the client database is present and in that database the client unique finger print are been present and along side the cell phone numbers also the fundamental data identified records. When the client put the finger on the unique model whenever the client puts the system automatically send the four digit code to the client associated with that data for the approval as it belongs to the client or not , client will access only by the code which is send by the system and to see if the client is substantial one or some one. Onyesolu and Ezcani (2012) they proposed the embedded biometric system for the Automated Teller Machine because they already found that the customers of ATM machine are very well aware of the ATM frauds with the help of the finger print and also with the card and pin it will provide the better security for the client

IV. MULTIPHASE SECURITY SOLUTIONS THROUGH THE LIFE CYCLE SECURITY

The fraud migrates form the geographical to but in the different and multiple direction across AM system comprising the multiple type of the security and physical security , ATM and security and also the network security. The objective of the life cycle security is to make the trust on the entire ATM system . It is exceptionally fundamental and important to consider security from the lifecycle

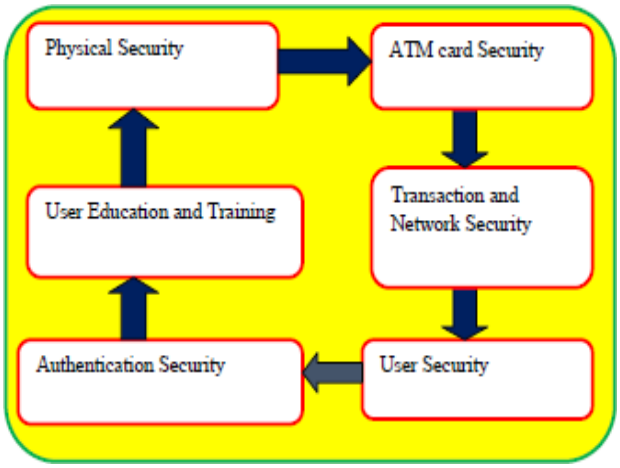

Fig 1. Lfe cyscle security of ATM system

The Auto mated teller machine system security life cycle refers that the all interlinked stages which are used for the functioning and which are used for operating the ATM from where and which fraudulent could target the attack in the system. The instrument chosen for the qualitative data collection are comprised in the four groups. Group 1 consist of the 3male/2 females , Group 2 consist of the 2 males/ 3 females, Group4 consist of 4 males/1 female, Group 5 consist of 5 males only, The group 1 and 2 are selected for the population of the students and the employees, group 3 and 4 are selected for the people who belong to the middle class and business persons, In the figure 1 it provides the security view point of the mobile banking, Hence the lot of money has been spent over the ATM system for maintain, The lifecycle security which is for ATM has a differs phases Physical, ATM card , Transactional , network Authentication , user, security.

V. ANALYSIS OF THE SECURITY MODEL

1. Strengths:

This system is difficult to hack and crack of security, It ensures that the ATM system is to be continued with trusted environment, It minimizes the risk of fraud and cancels out points of entry of the fraud into the operating system of the ATM as it has already trusted by the user , It also has the accuracy of the online banking through the ATM , It creates the security for the awareness of the end user, It having a very high user authentication security.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.115165

2. Weakness:

It requires the high memory and processor at Bank's servers, The transaction time increases and also has the lack of technology support , Lack of the trained security guard.

3. Opportunities:

It has the ability to obtain the large base due the higher security, growing popularity of the online banking through the channel of the ATM, It also consume the reputation of the technology and has a global expansion of banking services due the high in security.

VI. FLOW DIAGRAM OF THE SYSTEM

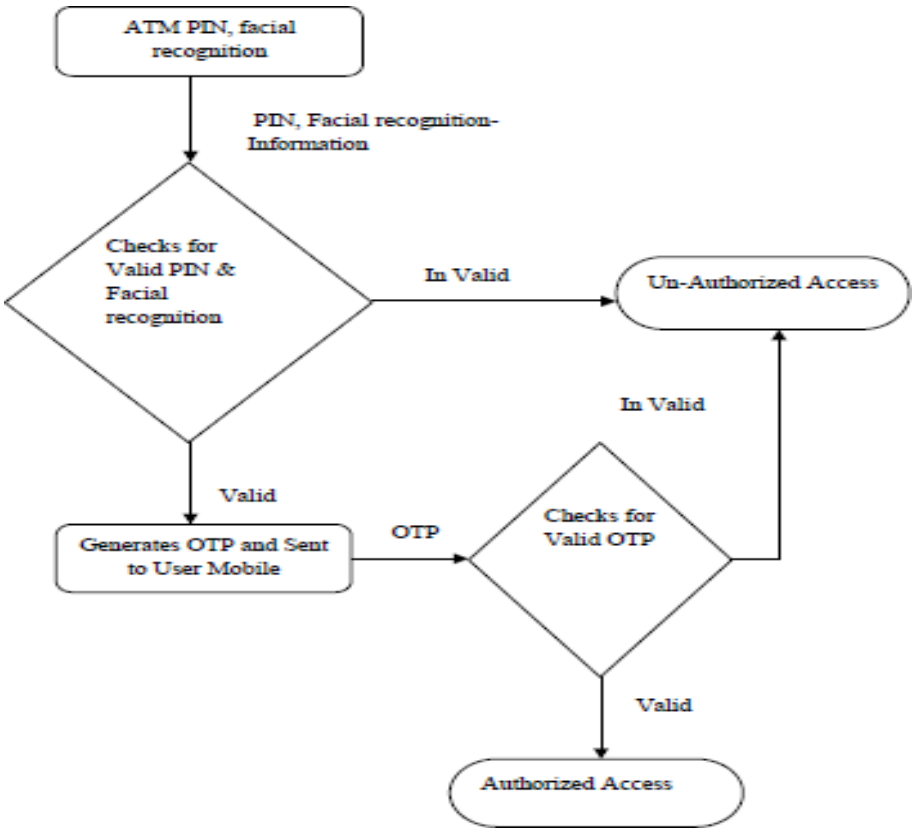

Fig 2. Flow chart

VII. CONCLUSION

The purpose of this paper is to investigate the threats of the security system in high level at all the phases along the life cycle accessing the crime migration risk of the pattern. There also a talk support for the fabricate applications for the ATMs that guarantee clients can safely exchanges at the ATM counters .The lifecycle of appears a series phases where the different kinds of protection are available at the different points along the life cycle to prevent fraud transactions and to reduce any type of risk.

REFERENCES

[1]. Lowlesh Nandkishor Yadav "Predictive Acknowledgement using TRE System to reduce cost and Bandwidth" Factor 7.39 Vol. 11, Issue 3, March 2022.
[2]. Vijay M. Rakhade "Reducing Routing Distraction in IP Network using Cross-Layer Methodology.
[3]. Shrawan Kumar Purve "A Survey on Packrat Parser."