A SMART CYBERGATE AUTHENTICATION FOR ERADICATING SKIMMER ATTACK IN ATM-CLOUD ENVIRONMENT

Dr.SAI

Dept. of Computer Science, St. Joseph's College(Autonomous), Tiruchirapalli, TamilNadu, INDIA

Dr.ECCLESTON

Dept. of Computer Science, St. Joseph's College(Autonomous), Tiruchirapalli, TamilNadu, INDIA

Dr.THOMAS FELDMAN

Dept. of Computer Science, St. Joseph's College(Autonomous), Tiruchirapalli, TamilNadu, INDIA

ABSTRACT

Advancements in digital technology perform tasks efficiently and conveniently. Automated teller machine is an electronic digital transaction system that has carried out various banking operations faster. However, Security attack is a major security risk in the banking sectors that cause big loss and also leads to bring down the global economy. Today, skimmer attack plays an important role on stealing cash from ATM by using pinhole camera and scanner through which collect all bank customer credentials with ATM PIN. To resist this type of skimmer attack, proposed security mechanism has developed an architecture for securing ATM PIN authentication in cloud environment. The contribution of the research work is that generates Instant PIN in the cybergate bank server by converting random number into ECC point by using Augmented Elliptic Curve Cryptography Algorithm that enhances high security in the ATM transaction system for eradicating skimmer attack in a secure way than existing cryptographic technique. High security, low computation cost, minimum storage space, efficient ATM computations, speed up banking operations, reduced response time, throughput and latency of ATM transactions can be ensured by proposed architecture.

Keywords: Cryptography technique, Skimmer attack, ATM transaction, Instant PIN, ATM security.

1 INTRODUCTION

As digital technology is developing day by day, there is need for protecting essential and privacy information of bank customer is a big concern in the global world. Especially, securing ATM transaction is a big challenge in the banking sectors. ATM is an electronic digital system that performs banking financial operations namely fund transfer, withdrawal and balance inquiry easier as well as faster [1]. Cloud computing is a technology where stores all secret information of banking operations, bank customers and render services to the account holder. The cloud computing model is used for performing efficient network access by using banking application, banking server, networks [3]. Three kinds of services are used in the banking transaction system for facilitating bank customer to utilize the bank services more conveniently. However, ATM security issue is a major security risk in the ATM cloud where stores bank customer credentials. Security ATM PIN has been hacked from ATM cloud by ATM security attackers that lead to breach the security in the banking field. Today, Eradicating vulnerable security attack is a major challenging task in the banking sectors [4-5]. Times of India Business Newspaper reported that recently one million debit cards have been robbed from India. Crime report has shown that skimming attack is a major banking security attack that takes place in the banking sectors. Skimmer attack is a major security risk in the way of stealing account holder details along with PIN by using pinhole camera and scanner. To combat this challenge, research work proposed Cybergate Secured Integrated ATM Cloud

Architecture for mitigating skimmer attack in the banking ATM system. It can protect the bank customer's secret data to fulfill the security requirements of ATM transaction.

2 LITERATURE REVIEW

The authors in [6] developed ATM Security model using security mechanism named as "Verification of control command" model. Secure ATM transaction model conducted three kinds of process in the ATM security transaction system. During the first stage of ATM process, Encrypting PIN Pad generated MAC1 with the request message and transferred to the Bank Server. At the second stage of ATM process, ATM bank server generated MAC2 along with reply message, after it was verified by MAC1 with request message and transferred to the ATM. At the time of third stage process, ATM dispensed cash to the ATM user after verification with the reply message. The limitation is that, there was no high security in the ATM transactions for eradicating skimmer attack.

The authors in [7] presented ATM authentication scheme with finger vein by using the concept of security techniques named as cryptography-steganography, machine learning. Bank customer details were encrypted by "Secured Hash Algorithm" and concealed encrypted data by covering image with the help of steganography technique. Secured bank customer credentials transferred to the ATM server where it carried out verification process for the authenticity of the customer by using cryptography and reverse steganography techniques. The machine learning technique ensured authentication system with biometrics that enhances high security in the banking operations. The limitation of this paper is to implement secure ATM system by using other security measures for better performance and user convenience.

The authors in [8] developed ATM security framework to carry out ATM transaction more efficiently using the SHA algorithm as well as Minutiae approach. At the first stage of ATM process, customer authentication was done by using cryptography technique. During the second stage of authentication process, fingerprint was processed through Minutiae approach and it was compared with the stored image using Euclidean distance matching technique. If it was verified, ATM permitted to dispense cash to the ATM user. At the third stage of the security process, Bank server generated OTP and sent to the user mobile through GSM technology. Once the user had entered the OTP within the time limit, ATM allowed to dispense cash. Otherwise ATM terminated the transaction process. The limitation is the lack of high security to protect ATM PIN.

The authors in [9] designed IoT based multi-factor authentication device along with fingerprint sensor, GPRS Technology and RFID technology which enhanced banking authentication in the banking sectors. A developed IoT device conducted a multi-factor authentication that includes ATM PIN, fingerprint biometric and One Time Password verification. A proposed banking authentication system in which RFID module carried out using electromagnetic to transfer account details between reader and card. Once the customer data and PIN had been verified, fingerprint sensor module executed authentication process with stored data. After verification process was done by these modules, the user was asked to enter OTP that was generated through PINENTRY device. If it was valid, it proceeded with the online payment process, otherwise it terminated the ATM transactions. The limitation is that there is no architecture proposed in this research works.

The authors in [10] developed a secure ATM authentication mechanism to ensure secured ATM transaction in the banking sectors. In the process of authentication, ATM user entered PIN, username in authentication application registered on smart mobile phone and send to the ATM bank server. If it was valid, it generated OTP and sent back to the custom based authentication application where it was stored. Once OTP had received by

authentication application, ATM user required to swipe their smart mobile phone by using the NFC card reader. If it was verified, ATM granted access to the user to get cash in a secure way. Future direction is to focus on security issues of custom based authentication application and also analysis is needed, to be performed on ATM security attacks.

AUTHOR	SECURITY TECHNIQUES	AUTHOR ANALYSIS	LIMITATION
[**Ogata *et al*., 2019]**	MAC Algorithm Security Technique	Proposed security model of control command verification was implemented by generating MAC to resist logical attack and lead to achieve authentication in ATM transaction.	There was no high security in the ATM transactions for eradicating skimmer attack.
[**Das *et al*., 2019]**	Cryptography and Steganography techniques	Developed security system eradicated security threats faced by ATM users in the way of verifying authenticity of bank customers and covering finger-vein image by using Cryptography and Steganography techniques.	Need to implement a secure ATM system by using other security measures for better performance and user convenience.
[**Manivannan *et al*., 2019]**	SHA algorithm, Minutiae approach and Euclidean distance matching technique	The proposed framework ensured secure authentication with biometric that was processed and verified user fingerprint by using Cryptography, Minutiae approach and Euclidean distance matching techniques.	The limitation is the lack of high security to protect ATM PIN.
[Cheng *et al*., 2019]	Multi-Factor Authentication Technique	Secured ATM system improved high level of authentication in the banking transaction process by using multi-factor authentication factors such as ATM PIN, biometric, OTP.	There was no architecture proposed in this research works.
[Mahansaria *et al*., 2019]	ATM authentication mechanism using NFC card reader	The proposed mechanism ensured secure ATM transactions using custom based application through which OTP was received and read with the help of NFC card reader to resolve ATM security issues.	Focus on security issues of custom based authentication application. .

Table 1. Security Techniques of ATM Network Functionality

3. PROPOSED METHODOLOGY

The aim of the proposed research is to develop a smart secured cybergate architecture for eradicating skimmer attack in ATM by using Augmented Elliptic Curve Cryptography Technique. The novelty of the research work is that IPIN is generated in the ATM - Cloud Security Server by converting random number into ECC point with the help of Augmented ECC algorithm that leads to increase high security than existing ATM security model with MAC algorithm. In this research work, IPIN is generated in the cloud that is a new way of securing ATM PIN along with bank customer credentials. As a result, it reduces high risk of security threats against skimmer attacker. Now-a-days, Bank customer has carried out ATM transactions that help to facilitate ATM users in terms of saving precious time, quick transactions. But there is a possibility of rising high security risk in the banking sector. This security threats have created a big loss for account holders. Skimmer attack is a major and frequently existing attack that enables hazardous hacker to create a duplicate ATM chip based card by using scanner and pinhole camera that can capture all essential information of the account holder. Hence, it is required to design smart secured cybergate architecture for eradicating skimmer attack to overcome this high risk of ATM security issues.

3.1 Key Features of Cybergate ATM Cloud Architecture

- Inhibits skimmer attack to facilitate ATM user to do transaction in a secure way
- Design for secured cybergate architecture to develop high security in the banking transactions
- Protects Instant PIN to enhance high security of banking ATM system by using random number generator
- Achieved IPIN authentication, non-repudiation, confidentiality and data integrity
- To proceed secured ATM transaction faster
- Minimum usage of memory space and low energy consumption
- Efficient computation of ATM transactions and Minimum response time of ATM transactions

3.2 Details of Network functionality for secured ATM transaction

Network functionality of secured ATM transaction is explained in the following steps:

Step-1 (ATM Functionality): ATM is an electronic device that executes ATM banking operations. On inserting card into card reader, it captures bank customer details and forwards it to the banking transaction appliction through which makes the request to the encrypting PIN Pad. It contains crypto-function where encrypt the account holder information with server public key by using Augmented ECC algorithm. The result is in the form of encrypted data that starts to send through banking transaction application from which forwards to the cloud gateway server via internet with router.

Step-2 (First Level of Authentication): In the MPLS Core Banking Network, Cloud Gateway Server collects encrypted data from ATM node through firewall and sends to the AAA (Authentication, Authorization and Accounting) server via MPLS technology. Proxy Server acquires requested data from ATM and processes the transaction. Decryption process can be conducted by the AAA server with server private key by using the same algorithm. Once authentication is done, authorization and accounting process takes place for checking whether customer is having sufficient balance or not. After validating this process, the next stage of testing is that verify the presence of any malware attack in the ATM transaction by antivirus server. If there is no malware program or software exists, it permits to transfer encrypted data to the Cybergate ATM Cloud Network Security Network.

Step-3 (Second Level of Authentication): In Cybergate ATM Cloud Security Network, web server has captured the authenticated data from cloud gateway server through cloud security broker with firewall and is shifted to the Cybergate Bank Server. It consists of authentication verification manager and key generation manager those who are responsible for contributing in the part of ensuring secure banking ATM transaction system. Authentication verification manager carries out decryption process with server private key using Augmented ECC technique. If key generation manager is received approval after verification test, then generates a secure random number that acts as Instant PIN by computing K_tN module. This random number can be created by using PIN and stored it in the banking ATM database and mobile user server.

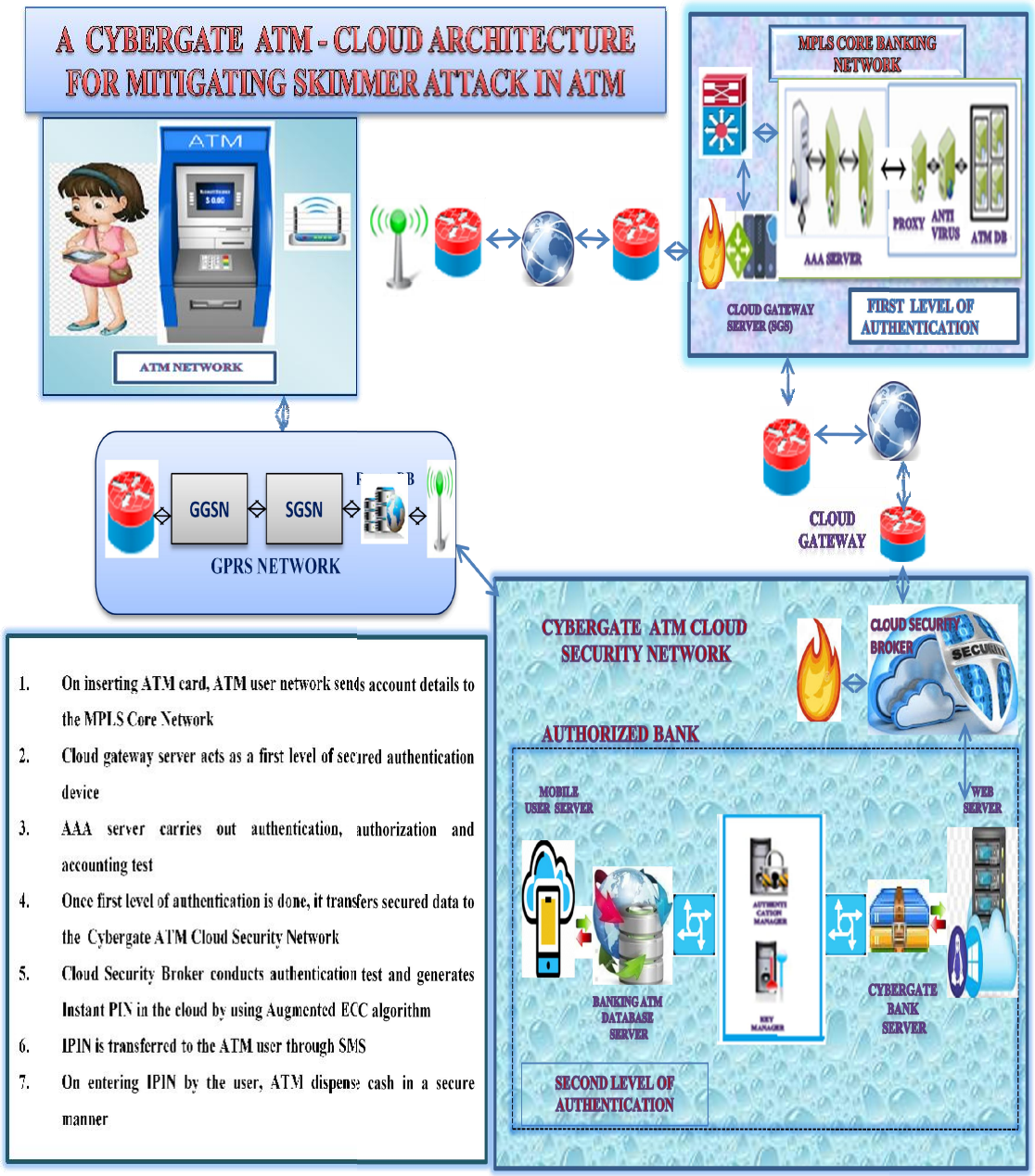

Figure 1. Cybergate ATM – Cloud Architecture

IPIN Generation: We have to consider prime number P, seed value K, point N. By using the mapping function with Augmented Elliptic Curve Cryptography, convert PIN into ECC point N. Now seed value K and point N is served as input into K_tN module. Outcome produces x_t and y_t points for 't' cycle as a result that is applied in the Equation (1) to create seed value for evaluating next cycle.

$$K_{t+1} = x_t + t(\text{mod } P) \quad (1)$$

We have to execute this process recursively until obtain the same pattern. The result is in the form of bit sequences that acts as Instant PIN. If there exits point at infinity, we have to calculate bit sequence by using an Equation (2).

$$K_{t+1} = y_t + t(\text{mod } P). \quad (2)$$

Same pattern occurs when it comes x_{t-i} where $(1<i<t)$ in the subsequent cycles that is $(x_t=x_{t-i})$. This random number is considered as Secure IPIN.

Step-4: IPIN Authentication

GGSN (Gateway GPRS Support Node) and SGSN (Serving GPRS Support Node) are important elements of the GPRS Network that provides message service to the registered mobile user. GGSN acts as a communication interface between external network and mobile network. GGSN obtains IP address of the registered mobile user and verify that user is active. If active means, it transfers data packet to the SGSN through GGSN. SGSN is responsible for validating the secure IPIN by using authentication technique and routing the packet to the ATM network through base station. If IPIN is received through SMS, user enters it within 90seconds. Then cybergate bank server verify that IPIN is valid or not by using random number. If it is, ATM permits to dispense cash without any security threats, otherwise it terminates from the ATM transaction.

4 CONCLUSION AND FUTURE WORK

ATM transaction system is an essential digital system that facilitates everyone to carry out ATM transactions efficiently. Combating the security issues against hacker is a big challenge in the ATM banking transaction. Now-a-days, skimmer attack plays a major role in the hacking of account holder details, fabricates duplicate ATM card to breach the ATM security. To tackle this kind of security attack, it is necessary to develop a secured architecture for stabilizing the high security. Proposed Cybergate Secured ATM Cloud architecture improves the level of security by using Instant PIN generated with the help of random number than existing MAC cryptography security mechanism. At the time of IPIN authentication, ATM user has entered IPIN that is received through SMS within 90 minutes. On entering valid IPIN by the ATM user, cybergate bank server is verified the authenticity of the ATM user using Augmented ECC algorithm. After validating IPIN, ATM permits to dispense money to the user. Otherwise it terminates the ATM transaction in the banking system. High security of the ATM transactions, minimum response time, low computational cost and expedite the ATM process can be achieved by the proposed architecture. Future work is that secured cybergate ATM – Cloud architecture will be implemented for eradicating skimmer attack to ensure secure ATM banking transaction.

REFERENCES

[1] Mridha M.F, Jahir Ibna Rafiq, Wahid Uz Zaman (2020) "Two Dimensional Hybrid authentication for ATM transactions, Journal of Advances in Data and Information Sciences, Springer Publications, January 2020.

[2] Ravi Kumar P, Herbert Raj P, Jelciana P (2018) " Exploring Data Security Issues and Solutions in Cloud Computing", 6th Conference on Smart Computing and Communications, Elsevier Publications, 2018.

[3] Chiraj Modi, Dhiren Patel (2018) "A feasible approach to intrusion detection in virtual network layer of cloud computing", Indian Academy of Sciences, Springer Publication, June 2018.

[4] Divyans Mahansaria, Uttam Kumar Roy (2019) " Secure Authentication for ATM transactions using NFC technology", International Carnahan Conference on Security Technology, IEEE publications, October 2019.

[5] Sweedle Machado, Prajyoti D'silva, Snehal D'mello, Supriya Solaskar, Priya Chaudhari (2018) " Securing ATM pins and passwords using Fingerprint Based Fuzzy Vault System", Fourth International Conference on Computing Communication Control and Automation, IEEE Publication, August 2018.

[6] Hisao Ogata, Tomoyoshi Ishikawa, Norichika Miyamoto, Tsutomu Matsumoto (2019) "Secure ATM Device Design by Control Command Verification", International Conference on Application and Techniques in Information Security, Springer Publications, November 2019, pp 32-50.

[7] Indrajit Das, Shalini Singh, Sonali Gupta, Amogh Banerjee, Md Golam Mohiuddin, Shubham Tiwary (2019) "Design and Implementation of Secure ATM System using Machine Learning and Cryto-Stego Methodology", Journal of SN Applied Science, Springer Publications, Volume 2, Issue 8, August 2019.

[8] Manivannan K, .Merline Peula D, Gayathri M (2019) "Elegent ATM Guarantee Framework using Minutiae Approach and SHA-256", International Journal for Trends in Engineering and Technology, April 2019.

[9] Xiaochun Cheng, Andreas Pitziolis Aboubaker Lasebae (2020) "Implementing Fingerprint Recognition on One-Time Password Device to enhance user authentication", International Symposium on Cyberspace Safety and Security, Volume 2, January 2020.

[10] Himadri Shekhar Mondal, Md.Tariq Hasan, Md.Mahbub Hossian, Md.Mashrur Arifin, Rekha Saha (2019) "A RSA Based Efficient Dynamic Secure Algorithm for Ensuring Data Security", Proceeding of International Joint Conference on Computational Intelligence, Springer Publications, July 2019, pp 643-653.