International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 12 | Dec -2016 www.irjet.net p-ISSN: 2395-0072

A- ATM: AADHAAR BASED SECURITY IN ATM

Abdul Rahaman Shaik[1],Vemuri Kusuma Priya[2]

[1]*Assistant Professor, Audisankara College Of Engineering & Technology, Gudur.*

[2]*Assistant Professor, Sree Venkateswara College Of Engineering,Nellore.*

Abstract: *In this paper, we implement a system securing the Transactions by user from Automated Teller Machines (ATM).We use AADHAAR related BIOMETRIC system to Authorizing the users. ATM allows the account holder to have transactions with their own accounts without allowing them to access the entire bank's database. Traditional ATM transaction method is replaced with this type of Biometric technology. With the use of this technology a genuine user can be identified, if incase of transactions made by some Unauthorized user then the that person's Aadhaar details has recorded . After identifying the user using its ID, then the user inputs ATM Pin number. If it is correct and his fingerprint is also verified then allowed to make transactions.*

Keywords: Phishing, Aadhaar linked Biometrics, key-logger.

1. INTRODUCTION

Today Internet has become major part of daily human lives. Online banking, online shopping etc are few examples of the today lives. With increase in the popularity of internet the importance of providing more security and authentication for online systems has also increased. In this paper we present one such security mechanism for ATM machines. Present technology used for ATM security is OTP which is easily crack able. Here we use Aadhaar linked Biometric mechanism which has linked with Aadhaar details. Along with normal OTP system, an additional finger print verification to ensure tight security.

2. ABOUT THE SYSTEM

In this to provide high security, we enhance the existing system with Biometric concept. Hacker may guess our password but he cannot escape from us because he should be make transaction with their Finger Print. If he make the transaction by his Finger Print then this finger prints has verified with this Aadhaar Details if it is matched his detailed has recorded . The major hacking threats like phishing, key-logger, shoulder-surfing attacks, and multiple attacks cannot affect our schema. After completion of biometric verification an Account holder receiving OTP via SMS. Even the OTP has also stolen by hackers , the details of the hackers who made the transactions has recorded. This method is more secure than the

traditional OTP system used today, because in this we provide Three-way security i.e OTP , Aadhaar Linked Biometric and ATM Pin.

The account creation is done by the banker which allows the user to register their Mobile number.. If the user put his card in the ATM then the Server validate the card and sent One Time Password(OTP) to registered mobile number and this ATM system asks user to enter their OTP . If OTP is entered then the system validating the OTP, if it is valid the system asks user to put his Finger Prints and this finger print data is direct validate with official Aadhaar details. If the data is found , it records the details of the user and time of transaction made by the user then the system asks user to enter his ATM pin. If this pin valid then system allows user to make the transaction. In case of unauthorized transactions, the Genuine Account holder make the compliant at his corresponding Bank then the bank authorities verifies the transactions details and they getting information about the person who made the transaction in that time. So it is very helpful to finding the hackers. Thus the user can proceed with the normal banking transaction. The main contributions of this paper are security improvements at a reasonable computation cost.

In addition, we incorporate an important function named recovery or change password allowing users to modify their passwords in case of need. The mutual authentication process is a combination of login and verification phases. Secondly we contribute in term of terms of performance analysis by analyzing the computation cost using different metric parameters such as: performance, random number generation in comparison with related works and finally we provided a security analysis in regard of known network and data attacks.

3. SECURITY ANALYSIS

***Confidentiality*:** In particular, these messages are confidential from any attacker.OTP should be sent to the mobile number which has registered in the banker's database. Even the attacker hacks our OTP by open air another Biometric is there to prevent him.

***Offline-password guessing attacks*:** The password guessing attacks are not feasible for our proposed system because it lacks a verifier table. the login phase, passwords and ids are not transmitted in plain text; instead, they are hashed and some operations are performed with them. they are transmitted with some other secret which makes it difficult for users to guess them.

***Securely change/update password*:** The proposed protocol help users change passwords at any time if they forget it or if they get hacked this password change facility provides robustness to the proposed improved protocol in comparison with a static password-based protocol.

***Session key establishment*:** This scheme provides session key establishment after the authentication phase. A session key is set up between the used device and the ATM for secure subsequent

communications. for each login session, the session key will be different and cannot be replayed after the time expires. Furthermore, the *user* and *system* can securely execute encryptions and decryptions by using of the session key and hence, achieve confidentiality for the subsequent messages.

In this the password maker solves all OTP related issues. It is a small, lightweight, free, open-source tool for internet explorer, firefox, google chrome, I phone, opera, php, windows, os/x, linux, flock, yahoo! widgets, android, python, and many other platforms & systems. it creates unique, secure passwords that are very easy for you to retrieve but no one else.

In our paper, the proposed system is an advanced ATM authentication system with improved security using biometrics. This Authentication system has three levels . The first level is a OTP generated by the server and sent to user's registered mobile number. The second level of authentication is biometric that is fingerprint. These two levels of authentication will provide enhanced security to the ATM system. The Third level is ATM pin number. The implementation is done as follows.

Banker's Task: The first is the login process. Initially the administrator does the account creation for a new user. Once the request is approved the user can open the account and an account number is provided by the bank at the time of registration. The login process of user leads to user page. The website provides the transaction details of the user, their account balance details about the bank and services provided by the bank.

*OTP Sending:*In this module the server generates a One Time Password(OTP) and sends it to the user's registered mobile number. The user inputs this OTP which enables him to proceed with the fingerprint authentication.

*Biometric:*In this module fingerprint of the user is enrolled and verified with Aadhaar Linked Biometric details. Fingerprint enrolment is done by UIDAI at time of Aadhaar registration for the person. Fingerprint is verified at the transaction time and if the fingerprint verified is valid, he/she can allow to withdraw the money and can check the account balance.

4. ONE TIME PASSWORD(OTP)

This Section presents the implementation of OTP Generation and how it can help in mitigating a typical phishing attempt. Whenever user wishes to do net banking, First step is to enter user ID and Pin number for User authentication. Once user is authenticated he initiates his transaction and gets the One Time password by SMS on his registered mobile number and a token is generated which is automatically stored on user's machine. Token with status value 1 is valid which signifies that OTP can still be used by the user. The moment user uses the generated OTP or after a *period of 5 minutes since user received the OTP on* mobile, the OTP expires and its token value changes

from 1 to 0. There is one more reason for generating token with OTP i.e. as it is stored on user machine it will authenticate that OTP has been sent through the primary web site by the same client who has initiated the transaction.

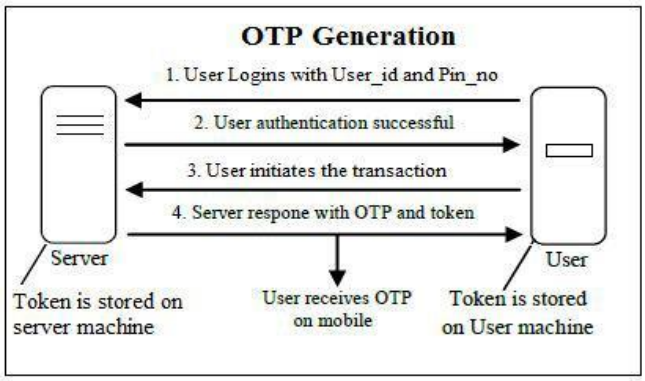

Fig-1: OTP Generation

When the user enters the OTP which he has received on mobile it is checked with server side OTP along with that, token value and its status is also compared for successful authentication. The cookie is valid only for 5 minutes and contains user machine IP address and other details. However, if attacker is able to get the user credentials by forged website (through Phishing attack), he/she will not be able to cause any damage as the transaction is not complete without OTP which is only accessible to the valid user as it is sent on the registered mobile phone.

5. FINGERPRINT TECHNOLOGY

For fingerprint recognition, a system needs to capture fingerprint and then follow certain algorithm for fingerprint matching. An improved enhancement algorithm of fingerprint image increase the security of bank account and the ATM machine. Fingerprint identification process consists of two essential procedures: enrollment and authentication. Fingerprint identification system compares the input fingerprint image and previously registered data to determine the genuineness of the fingerprint. If images of fingerprint are poor-quality images, they result in missing features, leading to the degrading performance of the fingerprint system. Thus, it is very important for a fingerprint. Recognition system to estimate the quality and validity of the captured fingerprint images.

Fig-2: Transactions Through Aadhaar Biometrics

In order to use an existing matching algorithm within the framework, the first thing that users need to

do is to create a resource provider. Resource providers allow saving (retrieving) to (from) files the resources associated with fingerprints. One of the goals that we kept in mind while developing this framework was to achieve class interfaces as simple as possible. This way, adding new algorithms is pretty straightforward. Also, fingerprint may be taken and digitized by relatively compact and cheap devices and takes only a small capacity to store a large database of information. With these strengths, fingerprint authentication has long been a major part of the security market and continues to be more competitive than others in today's world. Fingerprint recognition is an active research area nowadays. An important component in fingerprint recognition systems is the fingerprint matching algorithm. According to the problem domain, fingerprint matching algorithms are classified in two categories: fingerprint verification algorithms and fingerprint identification algorithms. The aim of fingerprint verification algorithms is to determine whether two fingerprints come from the same finger or not. On the other hand, the fingerprint identification algorithms search a query fingerprint in a database looking for the fingerprints coming from the same finger.

6. CONCLUSION

In this paper, we introduce a security system for preventing unauthorized access of a person's bank account by an attacker when the bank card is lost or when the password is stolen. The newly introduced authentication levels such as a OTP and finger print verification ensures tight security. This enables the authorized user to access his account securely and provides enhanced security to the ATM system. In future we can implements security by virtual session password along with new biometrics like as iris we expect it will be implement in future.

REFERENCES

[1] Secured Banking Transaction Using Virtual Password Krishnammal A1, Sindhiya S2, Dhivya P3, Janaki K4

[2] B. Ross, C. Jackson, N. Miyake, D. Boneh, And J. Mitchell, "Stronger Password Authentication Using Browser Extensions," In *Proc. 14th*

[3] ATM Security Using Virtual Password Renjith R1 , Arya S1 , Jasmine Yesudasan1 , Keerthy S Kumar1 , Krishnaveni S1 , Ajeesh S2 , Jooby E3.

[4] Securing SMS Based One Time Password Technique from Man in the Middle Attack Safa Hamdare, Varsha Nagpurkar, Jayashri Mittal.

[5] https://en.wikipedia.org/wiki/One-time_password

[6] http://www.explainthatstuff.com/fingerscanners.html

Mr. Abdul RahamanShaik has received his B.Tech Degree in Computer Science & Engineering from Priyadarshini College of Engineering & Technology, Nellore affiliated to JNTU, Anantapur, A.P in 2009 and M.Tech degree in Computer Science & Engineering from AVS college Of Engineering and Technology,

Nellore affiliated to JNTU, Anantapur, A.P, in 2013. He is dedicated to teaching field from the last 6 years. He has guided 4 P.G students and 10 U.G students. He is working presently as Assistant Professor in Department of Computer Science And Engineering, in Audisankara College of Engineering &Technology, Gudur, A.P, india.

Mrs. Vemuri Kusuma Priya has received her B.Tech Degree in Information Technology from Vignan's University, Guntur affiliated to JNTU, Kakinada,A.P in 2009 and M.Tech degree in Computer Science & Engineering from Mallineni Lakshmaiah Engineering College, Singarayakonda affiliated to JNTU, Kakinada ,A.P, in 2014. She is dedicated to teaching field from the last 5 years. She has guided 5 U.G students. She is working presently as Assistant Professor in Department of Computer Science And Engineering, in Sree Venkateswara College Of Engineering, Nellore, A.P, india.