iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** II **Month of publication:** February 2022

DOI: https://doi.org/10.22214/ijraset.2022.40534

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue II Feb 2022- Available at www.ijraset.com

Study on ATM with One-Time Password for a Safe and Smart Future

Chandana P[1], Khushi Sangani[2], Dr. A. Rengarajan[3]
[1, 2, 3]*School of CS and IT, Jain University, Bangalore*

Abstract: ***Money is the most crucial thing to accomplish nowadays, whether you're buying something, travelling, or dealing with a medical problem. However, it is inconvenient when you need to carry a significant amount of cash in your pockets. ATMs can in useful in this situation. The bank has an ATM that can disburse cash to you wherever you are. An ATM is a simple way to make money; all you have to do is insert a card and enter a PIN, and the money is yours. But, if someone steals your card and you know your password, he will have complete access to your funds. This highlights the issue of present security and necessitates the search for anything new in the system that can give a second degree of protection. A one-time password (OTP) is a password that is used to verify user authentication for a single login to a system. The security of the Automatic Teller Machine (ATM) system is addressed in this research in a novel way.***
Keywords: OTP, ATM, PIN, security, system.

I. INTRODUCTION

Standard ATM systems do not contain an OTP withdrawal feature. If the attacker was able to seize the ATM card / account number and PIN he could easily use it to withdraw money fraudulently. First, the user will be asked for the account number and ATM PIN, after which the user will receive an OTP on his / her registered mobile number. After logging into OTP, the user will be asked to withdraw or deposit. If he wants to withdraw - Now you need to log into the OTP system to withdraw money. So our system provides a completely secure way to conduct ATM transactions with security frameworks. To overcome the problems associated with the current ATM system, in our project we use a one-time password (OTP) system. Security has always been a major concern and protecting your integrity is the main goal of the entire organization. ATM is an IT-enabled Electro-mechanical IT system with connections to banking system accounts.

II. LITERATURE REVIEW

In contrast to passive attacks based on replaying collected reusable passwords, the system provides safe authentication for system access, login, and other applications that need authentication. The non-inevitability of the secure hash function ensures the OTP system's security. In the forward direction, such a function must be controlled, but inverting it is computationally impossible. The onetime password (OTP) based authentication system generates a sequence of one-time single use passwords using a secret pass-phrase. In this system, the user pass-phrase never needs to cross the network at any time, such as during authentication or password updates. External passive attacks on the authentication subsystem are protected by the OTP system [1]. The OTP one-time password system is run by two components. The generator must create the right one-time password using the user's secret password and information from the server's challenge. A job must be sent from the server that covers the right generation. The generator's settings must validate the one-time password received, save the last valid one-time password it received, and store the associated one-time password sequence number. The server must also make it possible for the user to change his or her secret password in a safe way. To create a one-time password, the OTP system generator runs the user's secret password, together with a seed received from the server as part of the challenge, though several rounds of a safe hash function. The number of secure hash function iterations is lowered by one after each active authentication. As a result, a unique password sequence is formed. By computing the secure hash function once and comparing the result with the previously accepted one-time password, the server authenticates the one-time password received from the generator. Leslie Lamport [2] was the first to propose this approach. Eavesdropping on network connections to get authentication information such as legitimate users' login IDs and passwords is one type of attack that occurs in networked computer systems. Once this information is collected, it can be utilized to obtain access to the system at a later date. This form of assault, known as a "replay attack," is addressed by one-time password systems [3]. Because no one should be able to guess the next password in the sequence, the security of the One-time password (OTP) system is critical. The sequence should be as random as feasible, surprising, and irreversible as possible [4]. OTP is a security feature that prevents unauthorized access to protected resources, such as a user account.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue II Feb 2022- Available at www.ijraset.com

The OTP method requires the user to enter a unique password for each login and is frequently used for two-factor authentication. The op system generator generates a one-time password by running the user secret pass-phrase and a seed supplied from the server as part of the challenge through several rounds of secure hash algorithms. The number of secure hash function iterations is lowered by one after each successful verification. As a result, a unique password sequence is formed. By computing the secure hash function once and comparing the result with the previously accepted one-time password, the server validates the one-time password predicted by the generator [5].

The OTP principle emphasizes that the method generates pseudorandom output each time the user attempts to log in, hence increasing security. A one-time password (OTP) is a password that is only valid for one login or transaction [6].

Bank robberies have become a global epidemic in recent years, affecting both clients and bank personnel. Many thieves use illicit methods to tamper with ATM cards and obtain access to client information. If the ATM card is lost and the PIN is taken, the attacker will have easy access to the user account, increasing the likelihood of an attack. People who opt to retain their PIN guessable, such as their birthdays, vehicle numbers, etc., will receive an OTP (One-Password Password) that will be delivered to the user's registered cell phone number, which the attacker will not be able to access. The importance of a one-time password security (OTP) system is that no one should be able to guess the next password in the series. The sequence should be surprising and irreversible, and it has been stretched as far as feasible.

The OTP approach, which is commonly recognized for two-factor authentication, allows the user to enter a new password for each entrance. As part of the challenge, the op system generator sends the encryption key and seeds acquired from the server to produce a one-time password using multiple duplicate safe hash functions. The amount of safe repeating hashes is lowered after each successful verification.

As a result, a one-of-a-kind password sequence is created. By computing the secure hash function and comparing the result with the previously accepted one-time password, the server confirms the one-time password that can be anticipated by the generator. The OTP policy stresses that the algorithm provides false output each time a user attempts to log in, hence boosting security. A one-time password (OTP) is a password that is only good for one entry or activity.

III. EXISTING SYSTEM

ATM allows users to complete basic transactions without using any banking operators. When a user inserts a card and enters a PIN there is no other level of security visible. If possible, the card is stolen and the PIN is broken by any attacker by slapping the shoulder, friends, participants, family, etc. once he has reached it there is no way anyone can stop him from stealing money from the bank. The current ATM system is not the safest system for the most important human assets namely Money. There is a need for a new system that is easy to get used to and very secure.

IV. PROPOSED SYSTEM

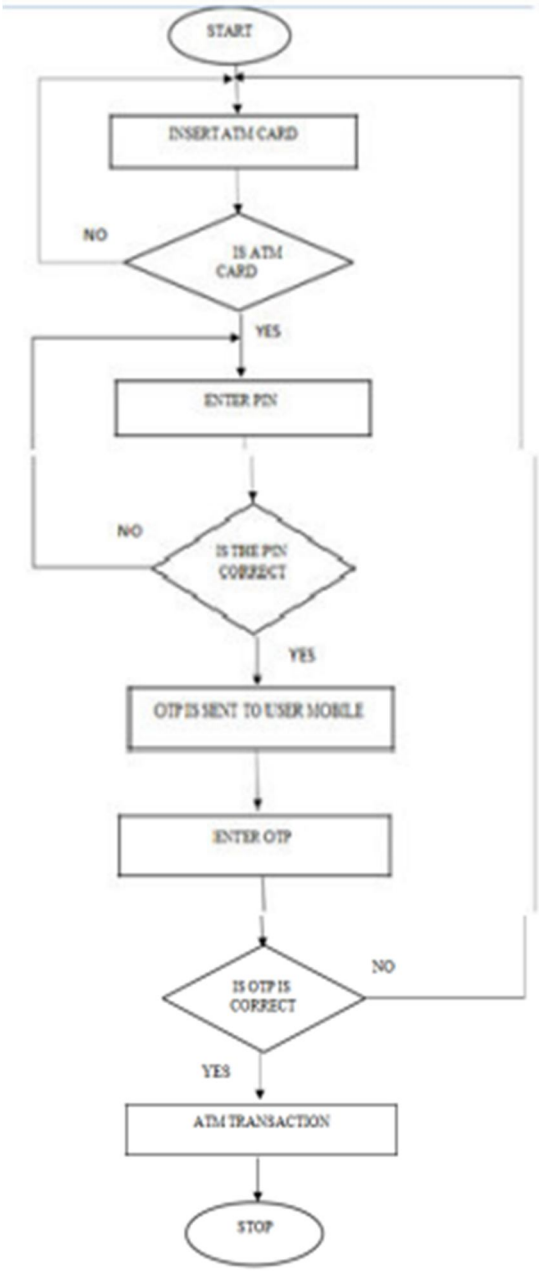
The goal is to provide secondary security to ATM systems, which may be accomplished through the use of OTP (Single Password), which is a secure and reliable method of adding protection to systems. The user's registered mobile number, which will be visible on the website, will get an OTP.

These applications provide the safest method of making ATM transactions. When a user inserts an account number into an ATM, the system asks for a PIN to verify the user's identity. OTP is produced and delivered to the user's cell phone number when the PIN number is validated. If the user enters a valid OTP, the operation will succeed; otherwise, the operation will fail. The card will be banned if the OTP setup is wrong beyond a particular threshold. The banking system will query about the user's cell phone number's mobile registration when the account is opened. For future reference, this information will be preserved on the bank's website. When a user visits an ATM machine, he must swipe his card into the machine, after which the machine and the bank server will check the card's verification and authentication.

If the card and its details are accurate, the machine will ask the user for his PIN. The card's information and PIN will be checked in the banking system.

The system will access user information from the website and produce an OTP, which will be delivered to the user's cell phone number when the cardholder and PIN have been verified. When a user receives an OTP code on their mobile device, they must input it on the screen in the same manner they would a PIN. However, there may be unforeseen consequences, such as a dead mobile phone battery, a lack of network coverage, or SMS delivery delays. If the OTP is correct, the ATM system will allow users to access their accounts.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue II Feb 2022- Available at www.ijraset.com



V. ONE-TIME PASSWORD

The ONE TIME PASSWORD technique is more efficient if the user wishes to authenticate the transaction at any time. The security of the OTP technique is critical because no one should be able to guess the next password in the series. The sequence should be as random as feasible, surprising, and irreversible as possible. Names, time, seeds, and other features can be utilized to generate OTPs.

1) *How OTP Works:* To implement OTP, we'll utilize a GSM modem to send an SMS (an OTP) to the user's phone number. People in rural regions have rudimentary phones that can receive text messages but no internet connections or e-mail capabilities, therefore they choose to utilize mobile phones over e-mail. We aim to employ mobile phones since they are plentiful, so that everyone may profit from the new suggested system. After the pin number has been verified, the user will get an OTP. After receiving the OTP, the user must input the 4-digit code. The user has three attempts to input the code. The account is temporarily stopped if the code is entered incorrectly three times in a row, and a notification is sent to the registered cellphone number.

2) Advantages of OTP

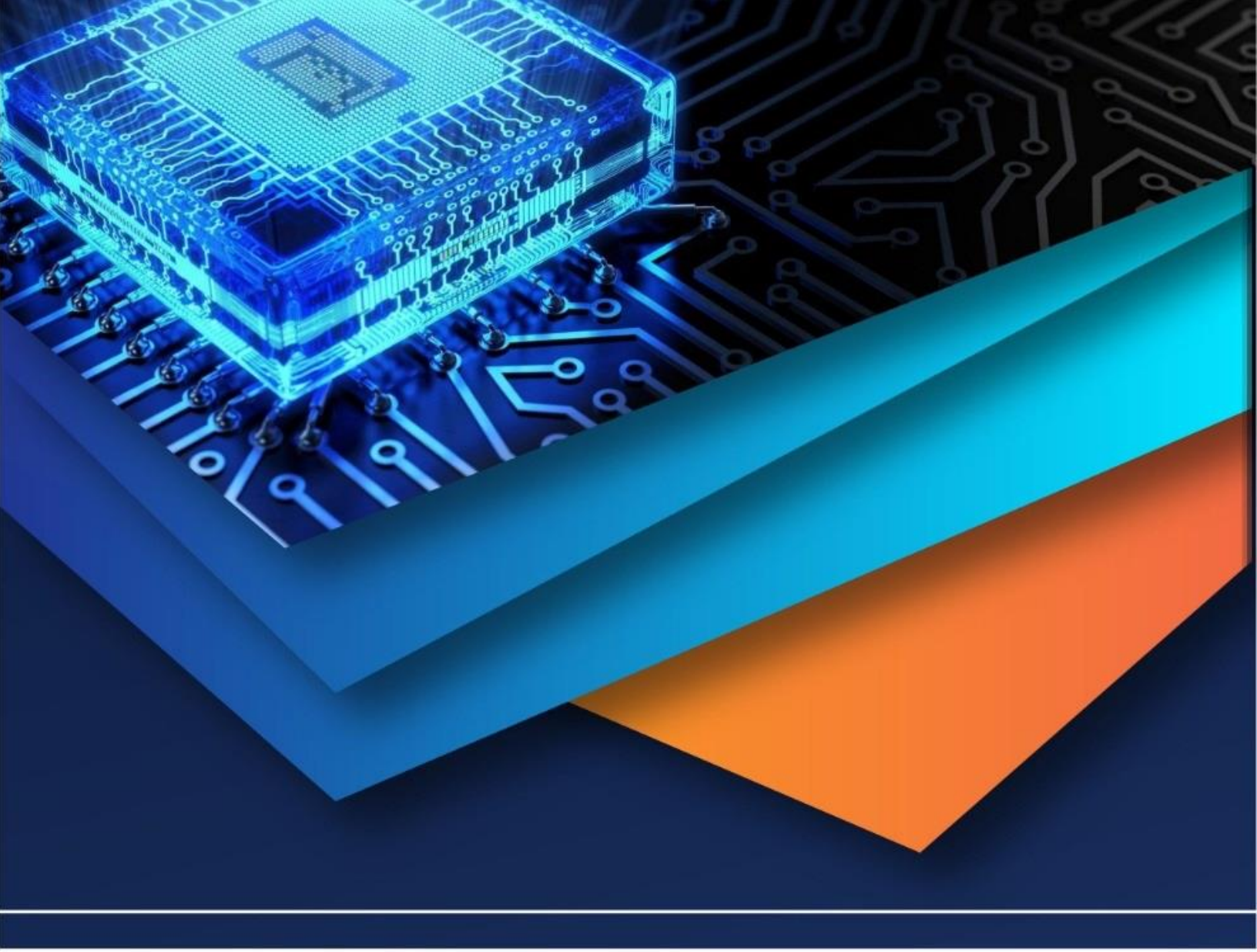
a) OTPs aren't subject to replay assaults because they're only good for one login.
b) Provides a more secure way to authenticate ATM transactions.
c) More improved security mechanism to keep you and your money safe when using an ATM.
d) In the event that your Card Number and PIN are compromised, this adds an extra layer of security.
e) OTPs are produced at random and are only valid for a limited duration, assuring maximum security.
f) SMS is the most cost-effective method of delivering OTP to the user.
g) Delivering OTP to a mobile phone is straightforward and safe because the user always has his or her phone with them.
h) To display the OTP, the user does not need to carry an additional device, such as a token.
i) SMS is well-known, has a large consumer base, and can reach practically every user.
j) SMS is supported by a wide range of phones.
k) It's completely free, safe, and simple to use.
l) OTP by SMS efficiently removes the need for users to generate and retain passwords, as well as phishers' attempts to crack passwords.

VI. CONCLUSION

The ATM system is currently a huge problem owing to security concerns, and it can also be hacked. Banks provide the customer with a four-digit PIN that may be altered at any time. The user generally changes the password after the first usage and maintains it guessable. This is a significant drawback of the PIN-type ATM technology. The best and simplest approach to cope with these security issues is to utilize OTP. The user's registered cell phone number will get the OTP. And that OTP will be used to get access to ATM transactions. Another major aspect of the proposed system is that it only needs modest modifications to the present banking and ATM systems. That means a small overhead will be needed to replace the entire system with enhanced security.

REFERENCES

[1] N. Haller, One-Time Password System, RFC 2289, February 1998.
[2] Leslie Lamport, "Password Authentication with Insecure Communication Communications of the ACM 24.11 (November 1981), 770-772
[3] Haller, N., and R Atkinson, "On Internet Authentication", RFC1704, October 1994.
[4] Reshma Begum, Dr. Basavaraj Gadgay, Veeresh Pujari, Pallavi B.V," Security of ATM System Using Biometric International Journal of Innovative Research in Computer and Communication Engineering (ijircce)
[5] N. Haller, C. Metz, P. Nesser and M. Straw, "A one-time password system", Internet Engineering Task Force requested for comments 2289, IEFT,1998.
[6] L. Lamport," Password Authentication with Insecure Communication", vol.24,1981
[7] Mohsin Karovaliya, Saifali Karedia, Sharad Oza, Dr.D.R. Kalbande," Enhanced security for ATM machine with OTP and Facial recognition features", International Conference on Advanced Computing Technologies and Applications (ICA CTA2015)
[8] Mohammed Hamid Khan, "Securing ATM with Biometric and OTP" International Journal on Recent and Innovation Trends in Computing and Communication, Volume: 3 Issue: 4
[9] S. Pooranachandran, E. Aravind, D. Bharathipriya, A.K. Gokul, E. Karthika," GENERATION OF SECURE ONE TIME PASSWORD FOR ATM SECURITY AND THEFT PROTECTION", International Journal of Advanced Research in Management Architecture Technology & Engineering (IJARMATE)
[10] S. Nithyanantham, Jamaludheen A, Dinesh Bhabu R, SuriyaRaja R, Sabari Raj S," Secure Based Single Time Authentication System, International Journal of Pure and Applied Mathematics, Volume 119 No. 10 2018, 1635-163
[11] https://ijesc.org/upload/590634167f500faaef802b6ad768e752.Secure%20and%20Smart%20Future%20ATM%20with%20One%20Time%20Password%20(3).pdf
[12] https://www.technoarete.org/common_abstract/pdf/IJERECE/v5/i5/Ext_90185.pdf
[13] https://www.jetir.org/view?paper=JETIR1503007
[14] https://www.sciencedirect.com/science/article/pii/S1877050915004093
[15] https://www.researchgate.net/publication/274142243_Enhanced_Security_for_ATM_Machine_with_OTP_and_Facial_Recognition_Features
[16] https://indjst.org/articles/enhanced-fingerprint-recognition-with-otp-using-delaunay-triangulation-to-improve-atm-security
[17] http://www.ijera.com/papers/Vol4_issue4/Version%205/N044057478.pdf



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY