IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 3, June 2023

ATM Fraud Detection

Prof. Rupatai Lichode[1], Muskan G. Chauhan[2], Ankita T. Chimurkar[3], Aditya N. Yerne[4], Girish V. Masade[5], Mayuri D. Tondre[6]
Guide, Department of Computer Science & Engineering[1]
Students, Department of Computer Science & Engineering[2-6]
Rajiv Gandhi College of Engineering, Research & Technology, Chandrapur, Maharashtra, India.

Abstract: Automated Teller Machines (ATMs) play a crucial role in providing convenient and accessible banking services to customers. However, the prevalence of fraud incidents in ATM transactions necessitates the implementation of robust security measures. This abstract explores the use of Time-Based One-Time Password (TOTP) authentication as an effective method for enhancing fraud detection in ATMs.

Keywords: Automated Teller Machines

I. INTRODUCTION

Fraud detection in Automated Teller Machines (ATMs) can be enhanced by implementing Time-Based One- Time Password (TOTP) authentication. TOTP is a widely used method for two-factor authentication(2FA) that adds an additional layer of security to the ATM transaction process. Traditionally, ATM transactions rely on a combination of a physical bank card and a PIN (Personal Identification Number). However, these credentials can be compromised through card skimming, PIN theft, or other fraudulent activities. TOTP authentication helps mitigate such risks by generating a unique, time-limited password that is required in addition to the card and PIN. The TOTP authentication process involves the following steps:

TOTP basically stands for Time-Based One-TimePassword in a subtle way. Many websites and services definitely require two-factorauthentication (2FA) or multifactor authentication (MFA) where the user actually is required to fairly present two or much more pieces of evidence: Something only the user knows, e.g.,password, passphrase, etc in a very major way. Something only the user has, e.g., hardware token, mobile phone, etc in a fairly major way. Something only the user is, e.g., biometrics, or so theyessentially thought. A TOTP value serves as thebasically second factor, i.e., it proves that the user for the most part is in possession of a device (e.g., mobile phone)that contains a TOTP really secret actually key from which the TOTP value specifically is generated, which particularly is quite significant. Usually theservice provider that provides a user's account alsoissues a sort of secret for all intents and purposes key encoded either as a Base32 string or as a QR code. This actually secret generally key essentially is for the most part addedto an authenticate or app (e.g., Google Authenticator) on a mobile device, showing how usually the service provider that

II. LITERATURE REVIEW

Fraud detection in ATMs is an important area of research, with many studies focused on developing effective techniques to prevent and detect fraudulent activity. Here are some key literature references on this topic:

"Anomaly Detection for ATM Fraud Detection: A Case Study" by K. P. Subbalakshmi and S. Senthil Kumar: This study proposes a technique for detecting ATM fraud using machine learning algorithms. The authors tested their approach on a real-world dataset and achieved good accuracy in identifying fraudulent transactions.

"Detecting Skimming Devices at ATMs Using Deep Learning" by M. T. Alam et al.: In this study, the authors propose a deep learning-based approach for detecting skimming devices at ATMs. They show that their method outperforms traditional approaches like rule-based systems and logistic regression models.

"Real-Time Fraud Detection in ATM Networks Using Machine Learning" by U. R. Acharya and R.

R. Joshi: This paper presents a real-time fraud detection system for ATM networks using machine learning algorithms. The authors demonstrate the effectiveness of their approach in detecting various types of fraud, including card skimming, phishing, and insider attacks.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 3, June 2023

"A Hybrid Approach for ATM Fraud Detection Based on Machine Learning and Rule-Based Methods" by F. Sedghi and M. Othman: This study proposes a hybrid approach for detecting ATM fraud that combines machine learning and rule-based methods. The authors show that their approach achieves high accuracy in detecting both known and unknown types of fraud.
"ATM Fraud Detection Using Data Mining Techniques: A Survey" by S. N. Panda and S. C. Satapathy: This survey paper provides an overview of different data mining techniques used for ATM fraud detection. The authors discuss the strengths and limitations of each technique and highlight areas where further research is needed.
Overall, these studies demonstrate the importance of developing effective techniques for detecting andpreventing ATM fraud. Machine learning algorithms and deep learning approaches are gaining popularity due to their ability to detect complex fraud patterns and anomalies in real-time

III. CODE

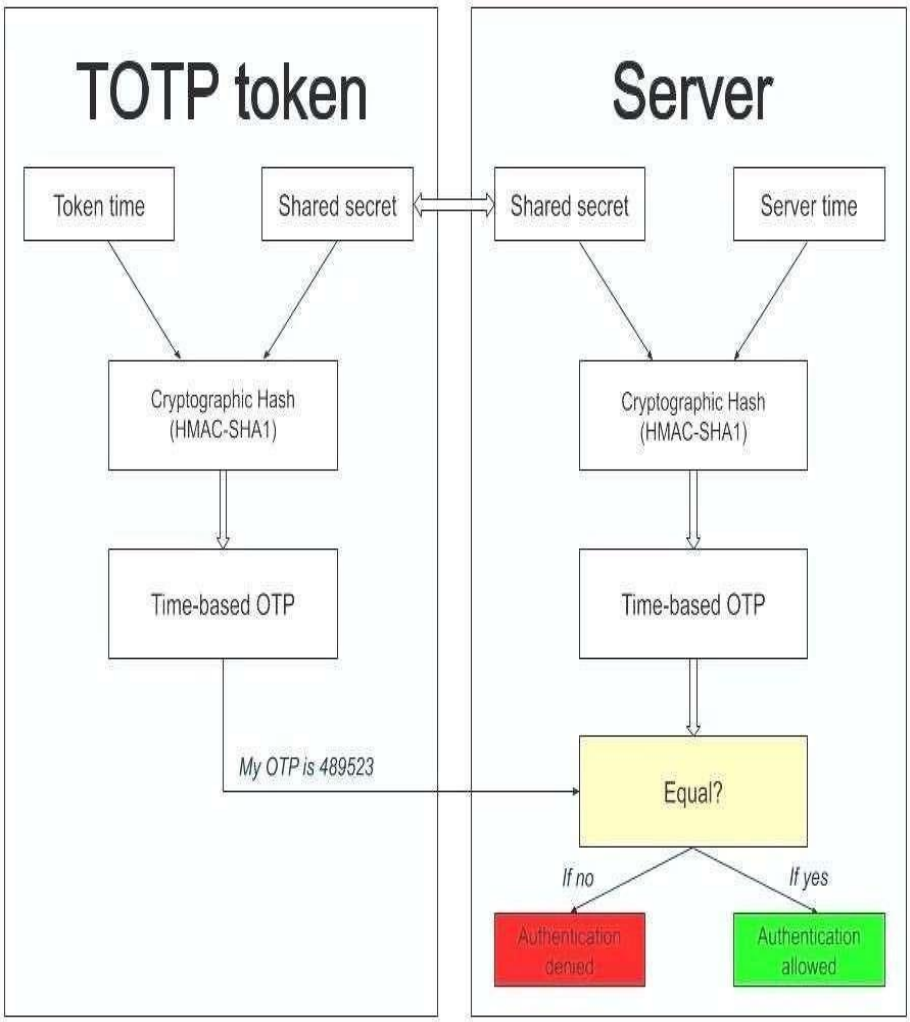
1}maintotp.py(pythonscript):-
#!/usr/bin/envpython3import base64 import hmac import struct import sysimporttime defhotp(key,counter,digits=6,digest='sha1'):
key=base64.b32decode(key.upper()+'='*((8-len(key))%8))counter=struct.pack('>Q', counter) mac = hmac.new(key, counter, digest).digest()offset = mac[-1] & 0x0f binary = struct.unpack('>L',mac[offset:offset+4])[0]&0x7fffffffreturnstr(binary)[-digits:].zfill(digits)
deftotp(key,time_step=30,digits=6,digest='sha1'):
returnhotp(key,int(time.time()/time_step),digits,digest)defmain():
args=[int(x)ifx.isdigit()elsexforxinsys.argv[1:]]forkeyinsys.stdin:
print(totp(key.strip(),*args))ifname ==='main':
main()

2}totp.sh(bashscript):-
#!/bin/bashecho "" echo""banner()
{
echo"+ +"printf"|%-40s |\n""`date`"
echo"| |"
printf"|`tputbold`%-40s`tputsgr0` |\n" "$@"echo"+ +"
}
banner"DevelopbyAkash,Piyush,OmandPrajyot"echo""echo ""
akash1(){read-p"Enterthe pathoffile:" path file=$(cat $path) echo $path >name.txtfor((;;))
do
python3mintotp.py<<<$file >otp.txtpython3mintotp.py<<<$file python3webhook.pysleep30
done} akash0()
{
piyush0(){read-p"GivenameforTOTP:" name echo $name > name.txt read -p"Enter SecretKey:"keyfor((;;))do python3mintotp.py<<<$key>otp.txtpython3mintotp.py<<<$keypython3webhook.pysleep30 done}
piyush1(){read-p"GivenameforTOTP:
"nameread-p"EnterSecretKey:"keytouch $name echo $name > name.txtecho$key>$name for((;;))do python3mintotp.py<<<$key>otp.txtpython3mintotp.py<<<$keypython3webhook.pysleep30 done}
read-p"WannaSave?enter{1}foryesand{0}forno: "numif[[$num= [10]]];then#validateinputpiyush"$num"
fi
}
read-p"HaveStored Key?enter{1}foryesand {0}forno:"numbif[[$numb
=[10]]];then#validateinputakash"$numb" fi
2}webhook.py(pythonscript):-

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 3, June 2023

```
importrequestsurl= "https://discordapp.com/api/webhooks/1048510542958051328/975qJHeLdq6xE80f7qdonN
FF8l0hosEWUNKw08KjqcA6mDG7xN5ehR1bywlZkfGu8qr"data={
"content" : "","username":"TOTP"
}
otp=open('otp.txt').read()name=open('name.txt').read()data["embeds"]= [
{
 "description":name,"title":otp
}
]
result=requests.post(url,json=data)try: result.raise_for_status()
exceptrequests.exceptions.HTTPErroraserr:print(err) else:
print("Payloaddeliveredsuccessfully,code{}.".format(result.status_code))
```

IV. UML DIAGRAM



V. FUTURE SCOPE

The future scope of fraud detection in ATMs using Time-Based One-Time Password (TOTP) authentication is promising, as advancements in technology and security measures continue to evolve. Here are some potential areas of development and improvement in this field:

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 3, June 2023

1. Biometric Integration: Integrating biometric authentication, such as fingerprint or facial recognition, with TOTP authentication can enhance security and further reduce the risk of unauthorized access. This combination of multiple factors provides a stronger authentication mechanism and makes it even more challenging for fraudsters to by pass security measures.
2. Machine Learning and AI: The application of machine learning algorithms and artificial intelligence techniques can enhance fraud detection capabilities in ATMs. By analyzing large volumes of transaction data, behavioral patterns, and historical information, these technologies can detect anomalies and identify fraudulent activities with greater accuracy. Ongoing research and development in this area can lead to more sophisticated and adaptive fraud detection systems.
3. Enhanced Transaction Monitoring : Future advancements in transaction monitoring systems will enable more comprehensive and real-time analysis of ATM transactions. Advanced algorithms can be developed to detect suspicious patterns, such as unusual transaction timings, frequent withdrawals, or inconsistent transaction locations, which may indicate fraudulent activities. Such monitoring systems can also leverage machine learning to continuously learn from new fraud patterns and adapt accordingly.
4. Risk-based Authentication : Implementing risk-based authentication can provide a dynamic security framework based on the level of risk associated with specific transactions. By analyzingvarious factors such as transaction amount, location, and customer behavior, the authentication system can determine the appropriate level of security required for each transaction. TOTP authentication can be dynamically applied based on the risk profile of the transaction, providing an additional layer of security when needed.

VI. CONCLUSION

- Biometrics, machine learning, transaction monitoring, risk based authentication, collaborative efforts, and continuous security evaluation. By embracing these developments, financial institutions can enhance the security of their ATM systems and provide customers with a safe and trustworthy banking experience.
- All in all, totp authentication is better than sms authentication. But while totp2 fais more secure than sms 2fa, it is not perfect. TOTP mfa is still susceptible to some types of cyber attacks. All the same, the lifespan of one-time passwords in totpworksto totp's advantage.