UPI fraud Detection Using Machine Learning

Sameer Kolekar, , Sourabh Panhale ,Dnyanendra Rengade ,Dipak Pawar
Prof. P.V,Kothawale
Dr J. J. Magdum College of Engineering, Jaysingpur,
Maharashtra, India

ABSTRACT

In recent years, banking through mobile banking and usage of debit and credit cards for transfer of money and purchases of goods has increased exponentially due to ecommerce and the introduction of Unified Payments Interface (UPI) by the government of India which allows user easy to use facility with minimal to no charges. To work this mechanism properly, a secure framework is required to avoid the risk of cyber fraud. there has been a great shortfall of security in banking applications in this type of transactions. This article presents a comprehensive study on banking security in e-banking by various techniques like blockchain, data encryption, voice recognition. This article explores the various security and technologies recommended by various researchers for safe and secure use of online banking.

Keywords—E-banking, Cyber fraud, Banking security, Voice recognition, Blockchain, Data encryption.

1.. INTRODUCTION

1.1. Background:

A Bank is a key part of civilization. It is a financial institution which deposits money given from the public and stimulates loan. Banks play a important role in the economic stability and development of the country. It is a Centralized system which is regulated by the respective governments of the states. the present model of banking can be traced back from the 14th century . There are different types of banks which are used for different purposes like retail banking, investment banking, etc.

1.2. Online Banking:

With the rapid increase in the advancement of the technology in the past few decades now banking services become online and more convenient as offline banking services become more time consuming and proved costly while compared to online banking. Due to the cheap cost of internet and the increase in the use of smart phones people are a common combination by connecting to a preferring to use the online banking rather than the traditional way for banking services. Government initiatives like introduction of unified payment interface system are also helped in increase in the use

of banking initiatives like this has encouraged a large number of clients to use remote banking.

1.3. Banking Security:

With the increase in the e-banking the security of banking has been subjected to various attacks and it has been proved that there is a great shortfall in the security of online banking. Most of the banking applications are using two factor authentication for verification now a day . For securing the banking and the banking services lots of research has been done so far. many researchers are recommending cryptography, biometric techniques, blockchain and secure transmission methods for the secure banking services.

2.EXPLORATION OF SECURED ONLINE BANKING METHODOLOGIES

One of the modes of communication that depends on wireless communication is the mobile, which utilizes a network of transmission towers that are spread out across a given area. The majority of these messaging services rely on Internet security and mobile network access security technology. The SMS's encryption using the Playfair Technique Instead than using single letters as in the simple substitution cypher and somewhat more complicated vigenère cypher systems then in use, the approach encrypts pairs of letters (digraphs). Only the portable devices and the cellular base channel's encapsulation terminal is used during transmission .

The new security primitive known as puzzle security and privacy issues which was created by using puzzle systems and is based on laborious ai riddles like sensory key systems this is a password system that combines a problem with graphics contrasting math analytics captcha with this will help to reduce the significance of captcha and achieve greater usability and data protection security professionals believe that AES is resistant to brute-force assaults a threat actor uses a brute-force attack when they try every key combination until they find the right one the size of the key used in encryption technique. This system offers enhanced protection and security that is highly accurate .

Mobile banking can provide 3A capabilities that are no longer constrained by time or space. With the maturation of mobile distance transmission technology and improved mobile technology capabilities, it will be capable of adding more substantially to the banking system. By implementing cutting-edge information and communications technology, moveable (mobile) banking, a new type of commercial facility importer, may offer customers effective and efficient production and economic. Mobile banking will be capable of contributing more substantially to the banking system if banks can integrate it with their current offerings, take advantage of the benefits offered by wireless communication technologies like cell phones, and create a single customerfocused services model .

In this method of CAPTCHA technique, OCR software can be used to extract data from the image. After learning about the security flaws in mobile and internet banking, it is crucial to implement security risk mitigation measures. Extended validation SSL certificates are replacing normal SSL certificates for encryption and digital certificates. login with a user name and password. The two-factor authentication methods, One-Time Password and CAPTCHA, give an extra layer of security to secure logins .

The risks associated with banking transactions make them one of the most important activities to support these transactions a secure mechanism is required less than 3 kb of ram are used throughout the encryption procedure and the overall delay is less than 015 seconds the average time to compress and decompress a message is 037 and 036 seconds respectively interceptors are unable to quickly access sms banking messages although there is a chance that attackers will succeed in obtaining the data it is presented as ciphertext making it difficult for them to decipher it the smart phone client is responsible for SMS message encryption whilst financial institution generates the encryption and maintains the document's cryptographic operations .

Identification and Compliance Risks, the login approach is among the cryptographic algorithms used in electronic wallets. By integrating a fingerprint reader into the programme, using end-to-end encryption to prevent data leakage, utilising behaviour analysis, and other methods, we may examine the security of banking services. Similar to the research methodology, which consists of three interconnected phases that describe the analysis environment, installation procedures, and necessary downloads for each mobile APK, such as the application, M-Banking encryption algorithm, Banker Implementation awareness and training, electronic fund transfer in Jordan, Electronic Security Audit, and Smart Android Review Kit are some of the terms that have been employed. Two mobile banking applications' overall security ratings indicated shoddy security procedures that urgently call for fresh clean. additional security concerns mentioned about most applications employ external drive for personal data. A study was conducted in an effort to supplement the earlier evaluations by focusing on Banking security concerns and the rise of malware and implementing a technique that uses both static and dynamic evaluation to identify security-sensitive and harmful app behaviours. To do this, a prototype was put into use for evaluation utilising a variety of apps gathered from Internet. After comparing the outcomes of the suggested ways for handling permission management on Banking, it was discovered there was only a one remote server .

A security seems to be a bond or another type of credit tool such is negotiable and has financial impact. For each transaction an OTP(One Time Password) was being routed on user , that is which you must then enter and confirm the transaction .It mean your information/ data is protected from all malware / cyber-attacks. Here are the some keywords which had been used so far "Mobile Banking, SMS Protocol, GPRS Protocol". Global System for Mobile communication as a standalone medium for transporting packet data without overlying integrity guidelines has proven highly susceptible to some security attacks Global System for Mobile communication statistics is vectorized, combusted, sending over a channel together with 2 different other torrents of metadata. We have provided solutions by enhancing existing bank integration, addressing issues with those implementations, and introducing two entirely new privacy controls for use with both short message service and Gsm network mediums .

The foundation of blockchain technology is cryptography. A dependable middleman carried out the transactions, and these third parties were in charge of carrying them out in a secure setting. The most appealing flexibility of blockchain technology for many industries, including banking, is its key selling point. The blockchain might reduce the need for middlemen, save costs, and boost revenue for the financial sector. As a private network, blockchain will operate on the Ethereum blockchain. The mobile phone app will use the LMK and the AES-256 method to encrypt the transaction text. With the use of blockchain technology, which has been incorporated into smart phones, users are now able to manage their passwords and other sensitive information. This algorithm has the capacity to detect and block such efforts.

To create safe mobile apps, Markova developed a methodology based on a service-oriented architecture (SOA).

The XML Key Management Specification (XKMS) framework for authentication and data encryption, as well as the RSA (Rivest-Shamir-Adleman) algorithm, are required by the model. An enhancement over the ElGamal encryption method is the Diffie-Hellman Integrating Encryption Method, which combines public key cryptography with symmetric key encryption hashing algorithms and MAC codes to create an integrated scheme. Nowadays, many individuals have a checking account and use cell phones, which are accessible to practically everyone, to handle their finances remotely. In the suggested system, a client must visit the bank and present the following data in order to create a bank account: a current e - mail address (or contact information), a backup email address (or mobile number), a primary password, and additional personal data. If the client is in danger, the backup e - mail and password are utilised. The bank will thereafter issue the customer a personal phone that is needed to verify ownership of the Account ala through the registration procedure SMS to a bank through short meassaging services allows the bank to receive the commands you submit text and images can be sent and recieved by MMS from a bank or customer they cam be run wirelessly and only required a brief linkage to the bank s system in order obtain information and complete a transaction.in this theis ,we have to maintain MMS based secure mobile banking with minimal cost using streganigraphy and cryptography methods .

3.Problem Definition

In case of the existing system the fraud is detected after the fraud is done that is, the fraud is detected after the complaint of the holder. And so the card holder faced a lot of trouble before the investigation finish. And also as all the transaction is maintained in a log, we need to maintain a huge data, and also now a day's lot of online purchase are made so we don't know the person how is using the card online, we just capture the ip address for verification purpose. So there need a help from the cyber crime to investigate the fraud. To avoid the entire above disadvantage we propose the system to detect the fraud in a best easy way.

4.Proposed system

In this system ,we present a hidden morkov model(AUTO ENCODER, LOCAL OUTLIER FACTOR, KMEANS CLUSTERING) Which does not required fraud signatures and yet is able to detect frauds by considering a cardholder's spending habit. Card transaction processing sequence by the stochastic process of an AUTO ENCODER, LOCAL OUTLIER FACTOR, KMEANS CLUSTERING.

The details of items purchased in individual transactions are usually not known to an FDS running at the bank that issues UPI Transactions to the cardholder. Hence, we feel that AUTO ENCODER, LOCAL OUTLIER FACTOR, KMEANS CLUSTERING is an ideal choice for addressing this problem. Another important advantage of the AUTO ENCODER, LOCAL OUTLIER FACTOR, KMEANS CLUSTERING based approach is a drastic reduction is the number reduction in the number of false positives transactions identified a malicious by an FDS although they are actually genuine . An FDS runs at a UPI Transaction issuing bank. Each incoming transaction is submitted to the FDS for verification. FDS receives the card details and the values if purchases to verify, whether the transaction is genuine or not.

The types of goods that are bought in that transaction are not known to the FDS. It tries to find nay anomaly in the transaction based on the spending profile of the cardholder, shipping address, shipping address.

5. COMPREHENSIVE ANALYSIS

1: DETAILED DESCRIPTION OF METHODOLOGIES PROPOSED BY VARIOUS AUTHORS

S.No	Authors	Brief Methodology Description
01	A. Abdulkareem [1]	SMS are encrypted using the Playfair Technique on mobile phone.
02	□. Beza□□□□□□	Advanced Encryption Standard (AES) algorithm for encryption of data and least significant bit (LSB) algorithm to hide the encrypted data in a image
03	M. Abdurohman [17]	ElGamal algorithm which is used to encrypt and decrypt the data using asymmetric key in SMS banking.
04	L. Nosrati & A. Massoud [9]	DES, Triple-DES, Blowfish
05	M. Fahim Naseri & Dushyant Sing [8]	Symmetric encryption algorithm AES and asymmetric encryption algorithm ECC.
06	K. Chikomo & A. Arnab	Security of the mobile banking performs the remote banking but security shortfalls in mobile banking
07	L. Nosrati [11]	Different Encryption Algorithms for Security of Mobile-Banking
08	J. Ibrahim [10]	Advanced technology and wireless technology users are more convenience to do their financial services through mobile banking security system. New technology has made people to access to the internet much easier.
09	N. Yildirim & A. varol [3]	Biometric recognition systems developed for mobile devices One-time password (OTP) and biometric features like fingerprint & voice or facial recognition must be used.

6. Challenges:

Technical obstacles, financial constraints and security concerns are all challenges. WAP proved to be too expensive and slow to satisfy the expectations of the consumer. People think about assurance.

Lack of a primary objective and a distinct institutional framework interfere with activity, causing a negative response in the network's internal and exterior parts.

The fact that costs outweigh advantages is biggest mobile banking's issue. The expense of key exchange prevents the growth of mobile banking in many nations.

7. DISCUSSIONS:

There are several types of encryption algorithms that can be used, each with their own strengths and weaknesses. Some commonly used algorithms include AES (Advanced Encryption Standard), RSA (Rivest-Shamir-Adleman), and Blowfish. The experimental results of the analysis of banking security methods revealed that the security in the banking application has been increased and less prone to the cyber-attacks and there is a improvement in performance of tasks in terms of resource utilization and time complexity. The experimental results indicated that the discussed algorithms and techniques could reduce the time processing of task by up to 15%.by using the machine learning technique we have able to improve the accuracy for testing the security of the banking application.

In most cases, end-to-end encryption is used to encrypt SMS messages. SMS messages are encrypted using a specific encryption technique, such as AES, on the sending device before being sent. The encrypted message is subsequently delivered to the receiver, who can then decrypt it using a key that was securely exchanged between them.

Risk Analysis: Analyzing the risks posed to banks by external and internal threats is essential for maintaining security in the banking sector. Risk analysis can help identify vulnerabilities and take preventive measures to reduce risk.

Authentication and Authorization: Authentication and authorization are two of the most important security measures for banks. Banks must use strong authentication and authorization measures to ensure that only authorized personnel can access sensitive information.

Data Encryption: Encrypting sensitive data is an essential security measure for banks. Data encryption makes it difficult for hackers to access sensitive information and can help protect the bank's customers.

Physical Security Measures: Physical security measures such as CCTV cameras and access control systems are essential for protecting banks from external threats.

Network Security: Network security measures such as firewalls and intrusion detection systems can help protect banks from cyberattacks.

User Education and Awareness: User education and awareness is an important security measure for banks. Banks must educate their customers and staff about good security practices and the risks posed by cyberattacks.

One of the main challenges with using data encryption is the management of the decryption keys. These keys must be kept secure and should only be accessible to authorized individuals, as anyone with access to the decryption key will be able to read the encrypted data. This can be a particular challenge in the banking industry, where there may be a large number of employees who need access to sensitive information on a regular basis.

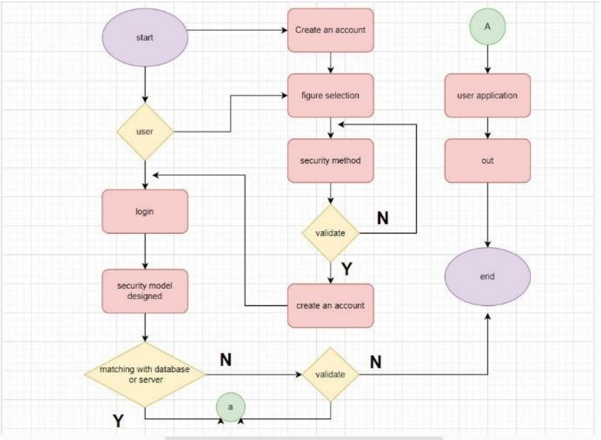

Fig. 1. Flow chart of banking system

Using banking services through online has become common these days which save the customers lots of time and reduces the need for physical visit for banks and also reduces the cost per transaction. To make this framework function properly we need to enhance the protection of the online banking so that In this paper we have gathered some of the important security features we can use for the improvement of banking security .we have discussed about using of voice recognition technique as a Authentication process and the implementation of blockchain technology to decentralization of banking system for the secure use of online banking and the cryptography for encryption and decryption of data to avoid the security breach

8. CONCLUSION

Our study's conclusion is that it's critical for E-Banking users to take precautions to safeguard their personal data and to be knowledgeable about any hazards involved with online banking. Using strong passwords that are only known to you, updating software and security protocols, and exercising caution when exchanging personal information or clicking on links from untrusted sources are some examples of how to do this.

Even with all the danger, there were still methods to succeed. We referred to it as security precautions. Physical access control, human aspect: awareness, and antiviral are examples of security measures. Limiting access connections to computer networks, system files, and data is facilitated by physical access control. Therefore, phishing scams can be avoided. Human aspect: By safeguarding our personal information and reporting the loss right away so the bank will repay your account, we can stop the criminal from carrying out his activity even if he is able to steal money from your account. Next, antivirus programmed have unique signatures that provide security and block access to harmful assaults.

9.REFERENCES

[1] Alharith Abdulkareem Abdullah and Wail Yas Nassir,"
Encryption of SMS Using Playfair Technique", ResearchGate 2014.

[2] Ahmad Salim1, Ali Makki Sagheer, and Linha Yaseen,"
Design and Implementation of a Secure Mobile Banking System Based on Elliptic Curve Integrated Encryption Schema",

[3] Nilay YILDIRIM and Asaf VAROL," A Research on
Security Vulnerabilities in Online and Mobile Banking Systems", IEEE 2019.

[4] Murad Obaid, Musbah Aqel, and Mahmoud Obaid," Mobile Payment Using Blockchain Security",2021.

[5] Raphael Olufemi Akinyedea and Odoseiye Aidohelen
Esese, "Development of a Secure Mobile E-Banking System", IJCRT 2019.

[6] R.Ganeshan, K Giri Kumar Reddy, V.S Manikanta and V Sai Lasya," AES Algorithm For Advanced Security In Online Bankin"(ISSN 2277-8616) 2020.

[7] Fatema Albalooshi, Yousif Albastaki, Max SmithCreasey and Muttukrishnan Rajarajan," Facial Recognition System for Secured Mobile Banking", ResearchGate 2018.

[8] Mohammad Fahim Naseri and Mr.Dushyant Sing," A
REVIEW OF MOBILE BANKING INFORMATION SECURITY AND PROTECTION METHODS IN AFGHANISTAN" IJCRT volume-6 2018.

[9] Leili Nosrati, Amir Massoud Bidgoli," A Review of Differenet Encryption Algorithems for Security of Mobile- Banking", IJETR volume-5 2016.

[10] Sameer Hayikader, Farah Nurafiqah Hanis binti Abd Hadi and Jamaludin Ibrahim," Issues and Security Measures of Mobile Banking Apps", International Journal of Scientific and Research Publications, Volume-6 2016.

[11] Leili Nosrati and Amir Massoud Bidgoli, "A review of Mobile Banking Security", IEEE 2016.

[12] Stuart J.Barnes and Barian J.C,"Mobile banking: Concept and potential", ResearchGate 2003.

[13] Amir Ghotbi and Nazanin Nassir Gharechedaghi,"
Mobile Banking, Challenges and Strategies in the Banking System of Iran", Journal of Basic and Applied Scientific Research 2012.

[14] Tibabu Beza, "Secure Mobile Banking Frame Work by Using Cryptography and Steganography Methods", GSJ: VOLUME-6,2018.

[15] Shaymaa Abdulla Al-Delayel, "Security Analysis of Mobile Banking Application in Qatar",2022.

[16] Kelvin Chikomo, Ming Ki Chong, Alapan Arnab and
[18] Andrew Hutchison "Security of Mobile Bankin", ResearchGate 2006.

[17] Yoso Adi Setyoko and Maman Abdurohman," SMS Banking Encryption Scheme", IEEE 2017.

[18] Nilesh Vitthal Limbore, "A STUDY OF BANKING SECTOR IN INDIA AND OVERVIEW OF PERFORMANCE OF INDIAN BANKS WITH REFERENCE TO NET INTEREST MARGIN AND MARKET CAPITALIZATION OF BANKS", ResearchGate
2014.

[19] Samir Pakojwar and Nilesh J Uke,"Security in Online Banking Services-A Comparative Study", ResearchGate 2014 .