Geofencing based Banking Authentication System: A Fraud Mitigation Technique

Kailash Kumar[1], Vikas Sihag[1]*, and Gaurav Choudhary[2]
[1]Department of Cyber Security, Sardar Patel University of Police, Jodhpur, India
[2]School of Computer Science and Engineering (SCSE), VIT Bhopal University, India
{spu17cs09, vikas.sihag}@policeuniversity.ac.in, gauravchoudhary7777@gmail.com

Abstract

In today's world of digitization, online electronic payment systems, and banking authentication have an important role in everyone's life. Banks use different ways of authentication at a different level to maintain the security of the hard-earned money. The security issues in the e-payment system, ATM, websites that store data or details of the cardholders lead to frauds, In ATM and POS transactions only card and PIN is been used and there is no other way of authentication. Researches purposed different methods such as Biometric methods which are hard to implement in the current scenario. There is no other authentication method in ATM and POS machine to authorize the user. In our purposed solution user will have his phone as an authentication device and we will get his location stored on a regular base and will only be able to make transactions when both the devices(Phone and ATM/POS)are in the same location this is called *geofencing*. This will help to track unauthorized access and will get the alert event when someone tries to access the account. It will help the investigation agency in case of fraud.

Keywords: Authentication, Banking Security, Geolocation

1 Introduction

The evolution of the internet has brought huge changes in the banking sector. Due to a rapid increase in technology and services in the banking system. All are connected with a single structure with the help of a core banking solution. In the current banking system, during money transmissions(inter-bank financial transfers) and transactions, the risk of fraud is high. User verification depending on multiple factors of authentication which is the initial step to the safety of online transactions.

- Something the customer can remember (passwords, PIN numbers)
- Something the customer keep (smart card, ATM cards,tokens)
- Something the customer himself (biometric characteristics such as fingerprint, Iris recognition etc)

We have discussed the types of frauds and methods of fraud detection, and improved authentication method for transactions. According to the definition of fraud by Reserve Bank of India [9]
"All instances whereby Banks are placing to lose through the deception of books of accounts, dishonest encasement of instruments like bills of exchange, unauthorized handling of securities charged to banks, cheques, drafts wrongdoing, stealing, conversion of property, cheating, shortages, theft, misappropriation of funds, irregularities, etc".

*Corresponding author: Department of Computer Science & Engineering, Sardar Patel University of Police, Security & Criminal Justice, Jodhpur Daizer, Mathania Road, Jodhpur-342304, India, Tel: +91-7728891698

According to RBI Over 23,000 cases of fraud involving a whopping Rs 1 lakh crore have been reported in the past five years in various banks.A total of 5,152 cases were reported from April,2017 to Mach,2018. [7]

Securely Authenticating customers required a variety of techniques and methodologies. These methods include customer passwords, USB plug-ins or other types of "tokens", personal identification number (PINs), digital certification using a public key infrastructure(PKI), biometric identification, physical devices such as smart cards, one-time passwords(OTPs), transaction profile scripts, and others. The risk factor in each method and technique varies.
More then one factor of authentication is difficult to compromise. Therefore, multiple-factor authentication is more reliable and fraud deterrent. Whereas, as ATM transaction required multi-factor authentication combined with a PIN. Fraudsters always have the upper hand so there must be regular improvement in the security of the banking system.

1.1 Problem Statement

In ATM, Skimmers are used to get the card details. while we use ATM we require Card and PIN if both are compromised and someone uses your card then transaction information occurs after money deduction from an account. further actions are taken afterward to track the fraudsters and it is hard to capture them. There should be an authentication system so that the user can get the information of his card used in ATM with his authentication only and only he can do the transactions. e.g In some cases in India even account holder doesn't have information about his/her account in bank and fraudsters with the help of bank insiders open account and use that account in malicious purposes. Customers do not have a way so that even after the ATM and PIN have been compromised they can be safe from frauds. They will come to know only after transactions are completed. They would not know if a transaction is been failed of someone try to initiate the same.

2 Banking Frauds

Frauds in Banks comprise of white-collar offenses as probed individually police. Banking frauds can be classified as Frauds by the insiders and by the other persons. It can be identity theft, vishing, SMShing, Money Mule, Trojan, Phishing, etc. These are the current type of frauds that are identified.

2.1 Frauds by insiders

- Rogue Traders:- It is an insider nominally authorized to invest sizeable fund on behalf of the bank and their employer. In such cases, they initially made large profits for their employers, and for bonuses for themselves.

- Wire fraud:- Wire threw in the sponge networks one as the international, interbank fund transfer system is becoming a target as there is a transfer of large money between different banks with the cheque and other methods this can be tampered by the insiders.

- Uninsured deposits:- There are cases in which banks are come out to be an uninsured or not valid one for deposition of money. so be aware while depositing money.

- Identity theft:- our information from the bank can also be leaked by the bank personals.

2.2 Frauds by others

- Tampering and stolen cheques - Cheques can be tampered and use and there can be a false signature on the cheque that can also be done.
- Accounting Fraud- To hide financial problems, someone can make a false account statement to hide the income, profits, and losses from the other or the government
- Credit card and Debit card Fraud- the maximum number of fraud are of these cards. where some can steal your card or take card details to commit fraud some methods to do frauds are:-
    1. Manipulation of genuine cards.
    2. Counterfeit cards are created with genuine cards.
    3. credit cards telemarketing is being done by Fraudulent.
    4. fraudulent applications are obtained with genuine cards.

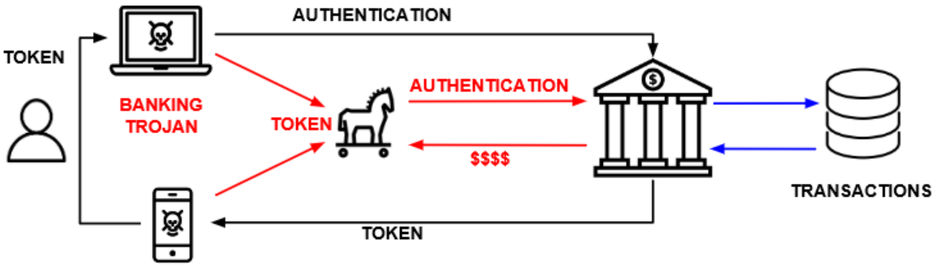


Figure 1: Typical Fraud Scheme: MitB and MitMo attacks
[3]

- Internet fraud and Phishing - Phishing is being done by sending a forged email, impersonating an online bank, auction, or payment site. the email redirects to the same looking webpage as of your bank and get your credentials and redirect you to the original website. There are numbers of malicious program that are been used such as “Trojan horse”, “spyware”, “malware” etc [2]

3 Authentication Systems

Security in the banking system aims to ensure access control, identification, and authentication.

3.1 Cheque Authentication

Paper plays an important role in bank documents. Therefore they are made with special papers made with cotton, grass, or bamboo.thickness for all the documents in the bank are different. even to improve the security different chemicals with fluorescent optical fiber are used which is visible in ultra-violet light. Banks use their watermark, color combinations for the document to improve the security. with these features it is hard to duplicate the cheque. [5]

Intaglio printing is used to print cheque that can be felt by touching. Some inks are thermochromic i.e they change color while exposed to heat. At the time of verification, the signature is been matched.

Banks have also launched an e-cheque by which you can create your cheque and send it by email.

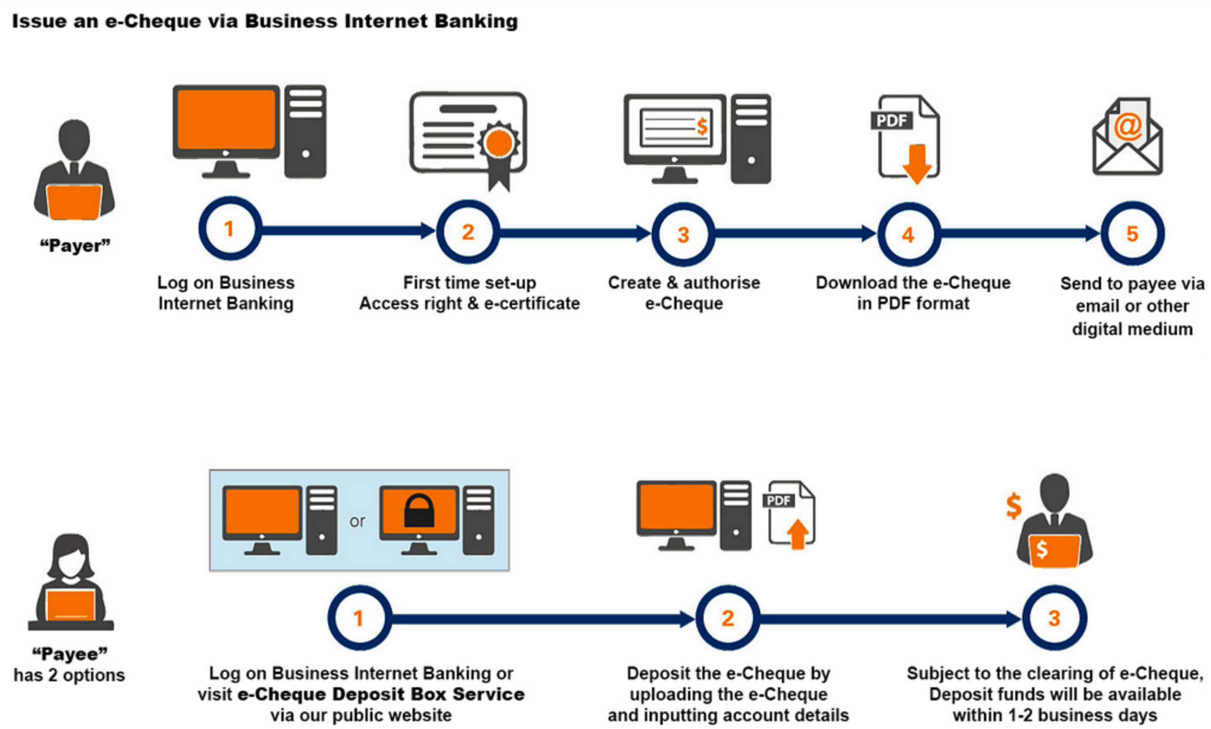

Issue an e-Cheque via Business Internet Banking
"Payer"
1
Log on Business Internet Banking
2
First time set-up Access right & e-certificate
3
Create & authorise e-Cheque
4
Download the e-Cheque in PDF format
5
Send to payee via email or other digital medium
"Payee" has 2 options
or
1
Log on Business Internet Banking or visit e-Cheque Deposit Box Service via our public website
2
Deposit the e-Cheque by uploading the e-Cheque and inputting account details
3
Subject to the clearing of e-Cheque, Deposit funds will be available within 1-2 business days

Figure 2: E - Cheque System [10]

3.2 Electronic Payment System

- One Layer Authentication Factor:- Basic factor of authentication that requires only user identity or data information.it can be compromised by the attackers easily. it includes user name, card-details, and many more.

- Two-factor authentication:- In this authentication contains pin, passwords, one-time password. The security level is increased but even then due to the lack of knowledge of users attackers steal all information with spam emails, calls, messages.

- Multi-factor authentication:- this is something you have. i.e biometric include fingerprints, signature, hand geometry, iris, face detection.

4 Banking Authentication System: Current Research and Progress

To enhance the digitization and security in banking sectors new methods and ways of authentication and fraud detection are being developed. We have focused on current research in multi-factor authentication which is under implementation.

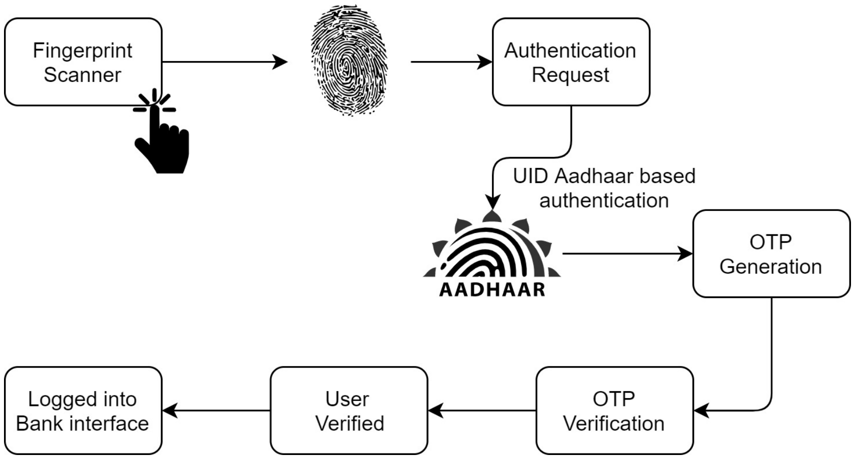


Figure 3: Online banking authentication

4.1 Biometric Authentications

Banks often use biometric based information for authentication in internal and external interfaces. Fingerprints are the most common biometric identity employed for authentication by banks.

- In ATMs:- Cards with PIN are standard authentication mechanisms for cash withdraw at ATM. A constrained-based approach can be used to reduce fraud. For withdrawing a large amount or an attempt for multiple transactions, biometric can be made mandatory. If withdrawing a small amount it may be avoided. Collecting and matching biometric for each request requires a sensor, which is open to dust, oil, and sweaty hands. Depending on the fingerprints of different persons, accuracy to collect and verify samples may be affected. [8]

- Online Banking:- As Banking accounts are linked with UID-Aadhaar in India users can also be verified by the Aadhaar biometric registration i.e by fingerprints. Banks can use it for authenticating users to access their online user interface (web or mobile) as depicted in figure 3. Authentication in the system is being done by biometric data which depends on the sample collected, reliability of the collected data, scanned data at the time of verification. Performance of which depends on False Identification and Rejection Rate i.e where a non-genuine entry is permitted and genuine entry is restricted [4].

4.2 Mobile-OTP with QR-code

Mobile OTP with QR-code and 2D barcode adopted internationally provides greater security, authentication, and convenience to the users. OTPs are classified as time-based One Time Password which is valid for a fixed short time interval and transaction-based. Event-based OTP is generated on an event such as being generated by a user or pressing a button on physical authentication devices. QR-codes are generated by the banks using the user's transaction information, the user reads the code from the mobile phone. The mobile phone generates the one time password which is to be transferred and hashed using the mobile serial number. Then the user enters the generated OTP code, to complete the transactions [6]. Secure mobile payment solution using QR code is popular amongst payment wallets such as Paytm, PhonePay.

4.3 Online-banking Authentication system Using Geolocation

The geographical location of a user may further strengthen authentication based on the user's behavior. Banks may use GPS or location-based services to identify a user's location and thus to authorize him/her for a service or not [1].

Using multiple positioning data from the cellular operator like Cell-ID, BSS, and other related data, the user's location may be identified to acceptable limits. The services using the location for various uses are known as *location-based services*. The location-based services use the built-in location tracker or the GPS to get location data from the user's device. It may comprise information such as:

- Longitude and Latitude details
- Device identification information such as IP address and hardware address.
- Transaction details.

Location based secure mobile banking:- Number of users using mobile banking facilities has increases drastically, thus security for the mobile phone is indeed important to have secure transaction. Mobile should be secure. Authentication credentials such as OTP must not be compromised. As banks have there mobile applications for banking purpose but indeed for all users it is not possible to have applications compatible to their devices, a location based secure browsing can be made available to user. A user can be authorized based on location attributes from it. Other device and browser identifiable information such as device id, hardware address and browser identity can be further used for backtracking the user transactions. It will ensure additional security checks to detect abnormal behavior.

5 Proposed Solution and Implementation

ATM cards are popular for cash withdrawal from accounts and for making digital payments on the Point of Sale machine(POS). Disclosure of card details and PIN using ATM skimming machines are common crimes in the cybercrime world. These details are used by cybercriminals to perform digital financial transaction from locations, which are not related to the actual card owner. To improve the dependency and without hardware change in the ATM or POS machine, we can make our transactions more secure by applying Geo-fencing that is restricting a user to initiate the payment only if they have their authentication device and ATM are in the same area. That will increases the level of authentication and user will also be notified even when a transaction is attempted or failed as illustrated in 4.

- Mobile Application:- It is used as a authentication device of the user to get the current location and login with the register mobile number with the bank. It take location, network information for accuracy.
- Database :- To authenticate user we have user Firebase which is a Google service to store real time database.
- ATM/POS machine :- A demo ATM/ POS machine is been created and linked with the database. It has a static location of the ATM as it can't be changed. It's location is been matched with a threshold with the real time location of the user using mobile application. This location matching is known as *geofencing*.

With the proposed system, messages of user activity would be send to user even in the case of failed transaction as illustrated in figure 5 and 6. Output of replicated terminal with different cases are shown below.

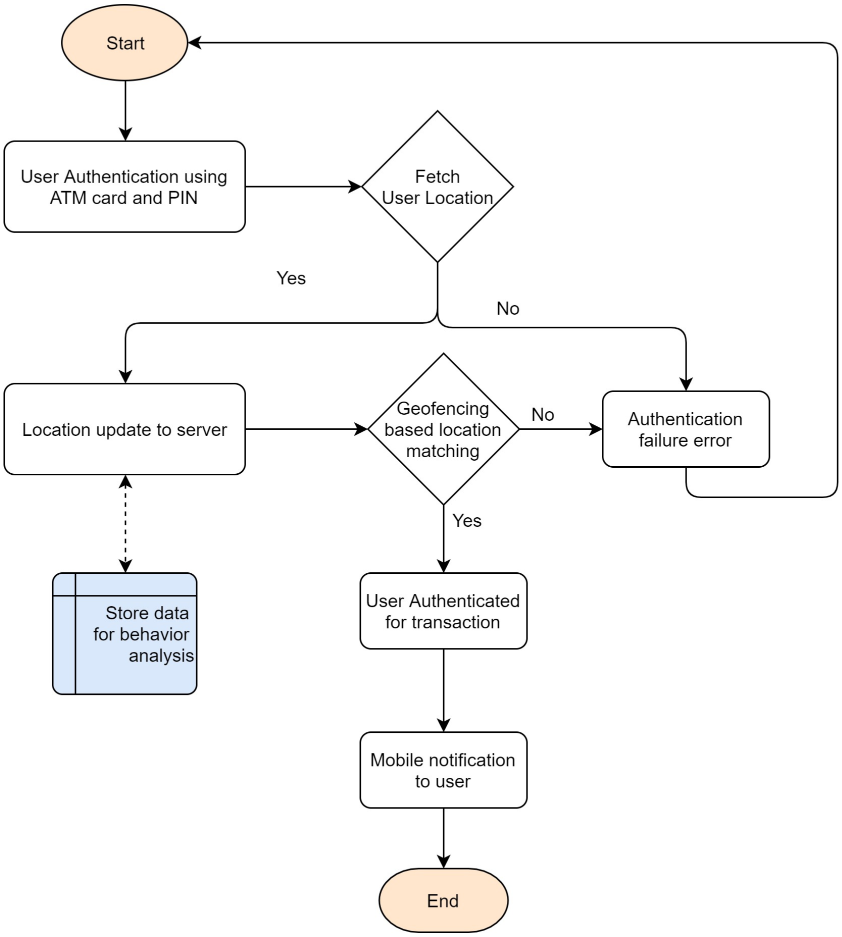
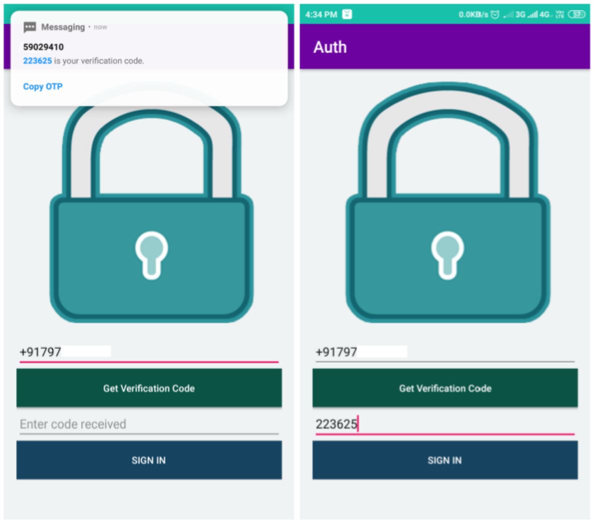

Start
User Authentication using ATM card and PIN
Fetch User Location
Yes
No
Location update to server
Geofencing based location matching
No
Authentication failure error
Yes
Store data for behavior analysis
User Authenticated for transaction
Mobile notification to user
End

Figure 4: Flow chart of the proposed system.


Messaging · now
59029410
223625 is your verification code.

4:34 PM 0.0KB/s 3G 4G 57

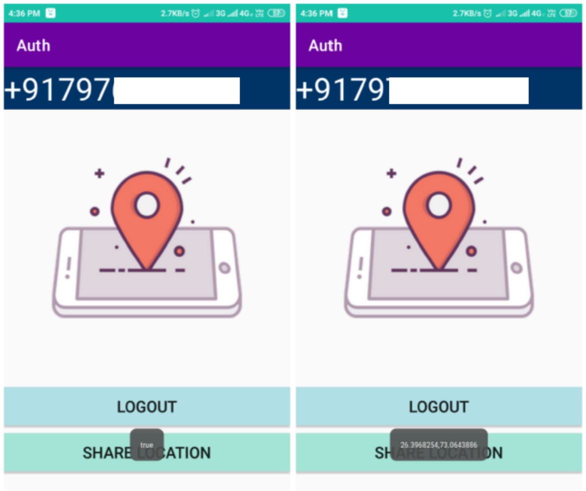
+91797

Enter code received

+91797

223625

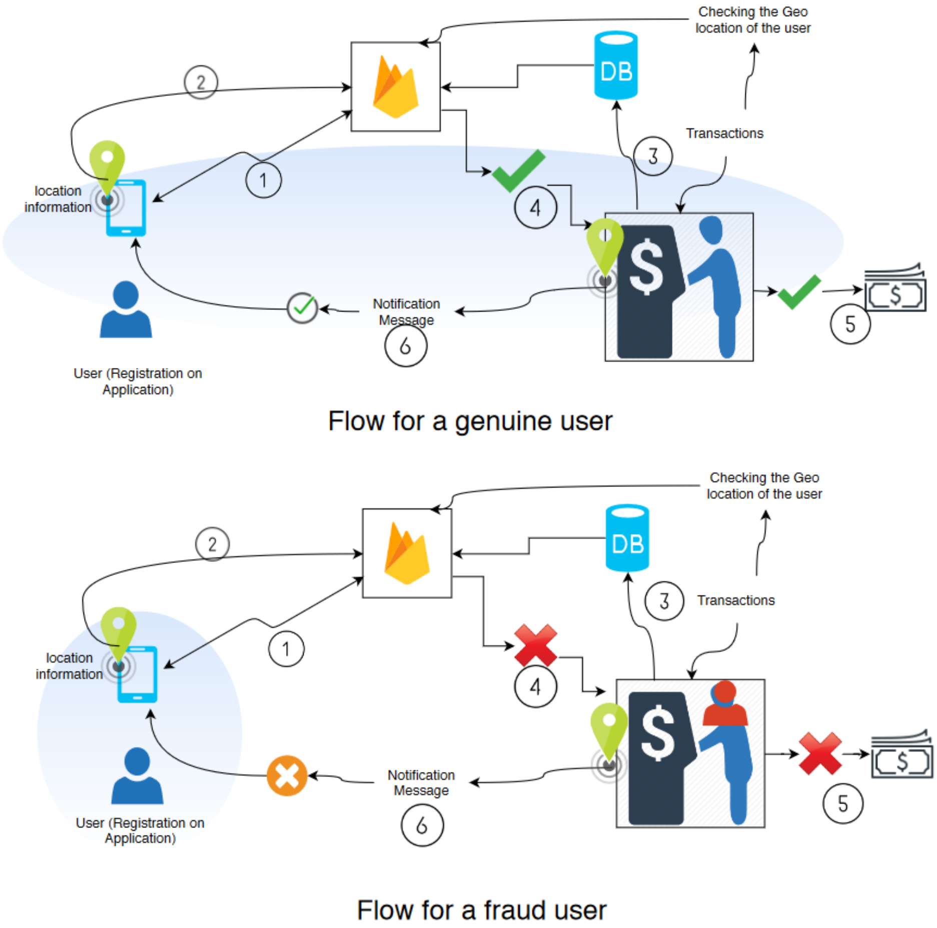
Figure 5: Screenshot of user being authenticated in mobile application using OTP.



true

26.3968254,73.0643886

Figure 6: Screenshot of user's location being sent to banking server for geofencing.


Checking the Geo location of the user
DB
2
1
location information
Transactions
3
4
Notification Message
6
5
User (Registration on Application)
Checking the Geo location of the user
DB
2
3
Transactions
1
location information
4
Notification Message
6
5
User (Registration on Application)

Flow for a genuine user

Flow for a fraud user

Figure 7: User interaction and working of the proposed system.

- *Case A* :
  ```
  If device is not in the range of ATM
  Enter Phone Number (included +91) in starting +9179***
  Enter Money to transfer 500
  Enter PIN 4 digit
  Auth device not in range.  It is 144.42 meters far.
  ```

- *Case B* :
  ```
  Device is in range of the ATM
  Enter Phone Number (included +91) in starting +9163***
  Enter Money to transfer 100
  Enter PIN 4 digit
  Auth Pass 100 Rupee transfer.
  ```

- *Case C* :
  ```
  Device is not integrated with the Geo Authentication
  Enter Phone Number (included +91) in starting +9194***
  Enter Money to transfer 500 Enter PIN 4 digit Phone Number Not integrated with
  Geo Authentication
  ```

Interaction of user with the proposed system and its working are illustrated in figure 7. For the proposed system to be integrated with existing banking system few changes would be required in mobile banking applications, ATM and PoS machines. Mobile banking application will be required to enable with the feature to capture the Geolocation in real-time data and matching it at the time of transaction. ATM and PoS machine will be required to be integrated with location sensors. To improve the security of the mobile banking application, it may be enhanced with device-binding and check for presence of a rooted device. Products for real-time fraud detection can be integrated to increase application and environment security.

6 Conclusion

Financial sector is always an attractive target for the cyber criminals. Recent cases of banking frauds has given rise to demand of an improved system which can detect frauds in real-time. Researches are working on new techniques of authentication and security of Core Banking System. Implementation and integration of additional security will provide banks to detect and prevent frauds. It will also provide law enforcement agencies crucial data for post fraud investigation. In this paper, we propose a banking user authentication system based on geofencing. User transactions at ATM / PoS are authorized based on user location context and geofencing. User location information will enhance location aware banking service delivery. User and banking system may be flagged for out of context abnormal usage behavior of the user. It will help bank and customer to improve and enhance the security of the ATM and POS transactions as well as tracking the users within the time for a fraud transaction.

References

[1] B. Akoramurthy and J. Arthi. Geomob—a geo location based browser for secured mobile banking. In *Proc. of the 8th International Conference on Advanced Computing (ICoAC'17), Chennai, India*, pages 83–88. IEEE, February 2017.

[2] M. Alemu and A. Omer. Cloud computing conceptual security framework for banking industry. *Journal of Emerging Trends in Computing and Information Sciences*, 5(12):921–930, 2014.

[3] L. V. Casaló, C. Flavián, and M. Guinalíu. The role of security, privacy, usability and reputation in the development of online banking. *Online Information Review*, 31(5):583–603, April 2007.

[4] P. Chatterjee and A. Nath. Biometric authentication for uid-based smart and ubiquitous services in india. In *Proc. of the 5th International Conference on Communication Systems and Network Technologies, Gwalior, India*, pages 662–667. IEEE, October 2015.

[5] R. Kumar and G. Gupta. Forensic authentication of bank checks. In *the 12th IFIP WG 11.9 International Conference on Digital Forensics (DigitalForensics'16), New Delhi, India, Revised Selected Papers*, volume 484 of *IFIP Advances in Information and Communication Technology*, pages 311–322. Springer, Cham, January 2016.

[6] Y. S. Lee, N. H. Kim, H. Lim, H. Jo, and H. J. Lee. Online banking authentication system using mobile-otp with qr-code. In *Proc. of the 5th International Conference on Computer Sciences and Convergence Information Technology, Seoul, South Korea*, pages 644–648. IEEE, October 2010.

[7] A. Mirchandani. Emerging challenges of indian retail banking: An insight into rising fraudulent practices in the banks. *International Journal of Finance and Quantitative Methods*, 37(2):1113–1120, April 2014.

[8] S. Singh, A. Singh, and R. Kumar. A constraint-based biometric scheme on atm and swiping machine. In *Proc. of the 2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT'16), New Delhi, India*, pages 74–79. IEEE, March 2016.

[9] S. Swain and L. K. Pani. Frauds in indian banking: Aspects, reasons, trend-analysis and suggestive measures. *International Journal of Business and Management Invention*, 5(7):1–9, July 2016.

[10] S. Yousafzai, J. Pallister, and G. Foxall. Multi-dimensional role of trust in internet banking adoption. *The Service Industries Journal*, 29(5):591–605, June 2009.

Author Biography

Kailash Kumar is a system security analyst at Housing Development Finance Corporation Bank. He is a security researcher having a keen interest in web application systems, malware analysis, fraud detection, and prevention methodologies. He has done a Master of Technology in Cyber Security from the Sardar Patel University of Police and a Bachelors in Computer Science and Engineering from Rajasthan Technical University.

Vikas Sihag has been an Assistant Professor with the Department of Cyber Security, Sardar Patel University of Police since 2013. He is also associated as a researcher with the Department of Computer Science and Engineering, National Institute of Technology, Raipur. He has received his Masters in Information Security from Motilal Nehru National Institute of Technology, Allahabad. His current research interests include Android security, malware analysis, digital forensics and protocol security. He is a British Standards Institution certified Information Security Management Systems - Lead auditor. He is also a CEH (Certified Ethical Hacker) and CEI (Certified EC-Council Instructor). He has organized various international and national training programs for Law Enforcement Agencies. He also has (co-)authored many journal/conference papers and book chapters.

Gaurav Choudhary received a Ph.D. in Information Security Engineering from Soonchunhyang University, South Korea. He has done a Master of Technology in Cyber Security from the Sardar Patel University of Police and received a Chancellor Gold Medal for Academic Excellence. He is presently working as an Assistant Professor in the School of Computer Science and Engineering (SCSE) at VIT Bhopal University. Before joining VIT Bhopal, he worked at Mobile Internet Security Laboratory (MobiSec Lab), South Korea as a Security Researcher on various projects funded by reputed organizations such as the Institute for Information and Communications Technology Promotion (IITP), National Research Foundation of Korea (NRF), and the Air Force Office of Scientific Research (AFOSR), USA. His current research interests include Threat Intelligence, IoT and CPS Security, Cyber Security, Vulnerability Assessment, 5G Security, Drone Security, and Cryptography. He has authored or co-authored many reputed SCI journal/conference papers and book chapters. He received the Best Poster Gold Award in WISA 2020, The 21st World Conference on Information Security Applications, Korea. He also serves as a Reviewer for various IEEE, ACM, and other journals.