2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)
Amity University, Noida, India. June 4-5, 2020

Security and Issues of M-Banking: A Technical Report

Priyanka Datta
Chitkara University Institute of Engineering and Technology
Chitkara University
Punjab, India
priyanka.datta@chitkara.edu.in

Sarvesh Tanwar*
Amity Institute of Information Technology
Amity University
Noida, India
*s.tanwar1521@gmail.com

Surya Narayan Panda
Chitkara University Institute of Engineering and Technology
Chitkara University
Punjab, India
snpanda@chitkara.edu.in

Ajay Rana
Amity Institute of Information Technology
Amity University
Noida, India
ajay_rana@amity.edu

***Abstract*— Now a day, Mobile banking playing a very vital role in everybody's life. Recently nobody has to stand in a queue at a bank counter for availing banking services since mobile banking had made it very easy. Sitting at a remote location using smartphone customers can avail banking services. It has many benefits; on the other hand, it has some demerits also. Hackers can easily trick bank customers using social engineering and cyberstalking to have their money. Cyber-criminals are hard to trace, so this opportunity is fully utilized by hackers. In this paper, a thorough review has been done on various types of scams that are taking place frequently on mobile or online banking. This paper mainly focuses on the increasing number of online fraud cases related to the banking industry. Hence, awareness programs are required among bank customers to prevent or avoid different types of online fraud..**

Keywords*— *Mobile Banking; Fraud on M-Banking; Online Scams; Digital Banking; Security of M-Banking

I. INTRODUCTION

Mobile banking means the bank will have a webpage through which it can almost provide all services of the bank to the customers. Customers sitting at a remote location using their smartphone or laptop can avail of services of the bank, like transfer of funds, recharge, payment, etc. As this application is very user-friendly so the number of users is also increasing [1]. Recently banks with mobile or net banking are experiencing very complicated online services since digital privacy and security are of high alert. Therefore banks are required to provide more secure and safe online banking services [2]. Identity thieves, money launderers and hackers are focused on various channels and creating new types of attacks so that they cannot be easily trapped by traditional fraud detection systems [3]. Bank customers are now using fewer services of online banking since the number of fraud cases are increasing[4]. To overcome this problem awareness programs are required for bank customers so that in future online scams can be prevented.

This review paper is organized as follows: Section II consists of Motivation of the paper followed by Section III Literature Survey. In Section IV Outcomes of the Survey are discussed. Finally in Section V conclusion of the paper is given.

II. MOTIVATION

Banks industries are playing a very crucial role in organizing and channelizing the money of the country. But, recently they are facing a crisis since the number of online fraud cases is increasing speedily. For example, Indian banks had lost Rs. 109.75 crores to online and theft fraud in the financial year 2018 [5].

The above report motivates us to review different types of mobile banking scams due to which fraud cases are increasing in the banking industry.

III. LITERATURE SURVEY

The following section illustrates the related work on mobile banking fraud done by various researchers.

Modi and Dayma had presented a comparative study of various techniques of online financial fraud had been detected. Different methods used to detect the fraud are the artificial neural network, Hidden Markov model, decision tree, rule-based method and convolutional neural network. The advantages and limitations of these methods are also illustrated. Finally, it had been concluded that either single method or combination of the methods with some add-on new feature can be used to detect the fraudulent transactions [6].

John et. al had addressed the detection of bank fraud with the help of data mining methods like clustering, association, classification and forecasting for analyzing customer data to detect patterns that can cause fraud. After identifying the patterns, a more secure level of verification or authentication can be added to the process of online banking [3].

Madan Lal Bhasin had suggested that banks can preserve and secure the safety, authenticity, and integrity of online transactions by deploying scrutiny at multipoint through checking hurdles using cryptography. Bank employees working at the sensitive areas should be rotated at a regular interval, as well as technologies should be updated periodically. A bank can able to detect fraud very quickly by leveraging the technology of data analysis. Though 100% of secure banking cannot be achieved for unknown threats a certain level of precaution can be taken to minimize the risks [7].

Parul Deshwal had examined the bank's customers' adoption of mobile banking and its merits and demerits factors that influence the adoption of digital banking by Indians. There is a requirement for generating awareness program regarding mobile banking among peoples so that they can use it for their benefits [8].

978-1-7281-7016-9/20/$31.00 ©2020 IEEE

Emad and Salam had presented security and challenges issues along with their characteristics about internet banking. Some strategies for fraud detection, various types of attacks and their prevention methods adopted by the electronic banks are discussed. According to the authors, the model which is most effective is "Transaction Monitoring" and on the other side the models which are worst effective are "Device Identification", "Browser Protection" and "Virtual Keyboards" according to the respondents' opinion [1].

Mhamane and Lobo, the objective of their paper were to prevent and also detect fraud related to mobile banking with the help of algorithms like the Hidden Markov Model (HMM). It had also ensured that authorize transactions are not denied through the use of OTP (One Time Password) send to the registered mobile number of the customer. Banks are seeking for prevention system that can minimize the huge amount of losses due to fraud. As there has been no effective model for detecting unauthorized users and tracing their unlawful activities is very difficult. Authors had proposed a system for overcoming these difficulties using HMM [9].

Nie and Hu had presented issues on the information security of internet banking. This paper discussed various protection measures on security like identity authentication, encryption technology, wireless public key infrastructure (WPKI) technology, and digital signature [10].

Vasilis Aggelis had demonstrated a successful model of fraud detection which was established in Greece. The brief discussion had been provided on offline fraud detection system for internet banking, the aim of this paper was to present its input in reliable and fast detection of any unlawful transaction [11].

IV. OUTCOME OF THE SURVEY

After reviewing various research articles and newspaper regarding online banking fraud cases, helped us to identify various important factors behind the cause of increasing online fraud cases. Foregoing section analysis the results obtained during the survey.

A. Different types of Online scams are as follows:

1) Phishing email scams: The Internet can be a dangerous place. One common technique scammers used is "Phishing". Criminals use to send out seemingly authenticate emails directing users to a website. Once the users move to the website, scammers use various types of tricks to convince users and reveal their personal sensitive information. Scammers may also send an email with an attachment, like a word document or zip file. When the user downloads the attachment, malicious software is installed on their computer. Through this software, scammers get access to the user's computer and capture vital and sensitive information [12].

2) The Nigerian scams: In this type of scams usually, the victim received emotional messages, social networking message or emails from scammers to help them for retrieving a huge amount of money. They also assure that after recovering the money, they will provide some percentage to the victims also. Those who trust such messages or email, they lost their money instead of gaining [13].

3) Greeting card scams: During festivals, we often received an email with greeting card attachment. It seems to come from a person who cares about us, but actually, the scenario is quite different. In reality, scammers send those emails, if we download the attach greeting card then malicious software automatically installed on our system. Now, through the malicious software scammer get the access of our system and also to the vital information like banking credentials [14].

4) Credit card or Bank loan scams: Sometimes user received email as if it has been sent from some big known company. The email states that the user had owned a lottery of a huge sum of money, to avail the money it requests for some banking information. It also asked to pay some money for processing the lottery and as a banking service charge. If the user trusts such email and shares banking details with the money too, then the user is victimized of Bank loan scam [15].

5) Hitman scams: Criminals asked victims through email to pay some amount of money with the help of online banking. They threatened that if the victim doesn't pay the money then they will harm their near ones. It provides some victim's personal information along with the email, to assure the victim that there is a real danger ahead. To avoid this hitman type of scam, we should not post sensitive or valuable personal information on social media [16].

6) Online romance scams: Everybody is using Facebook or Instagram applications daily. Likewise, dating applications are also accessible which guides boys or girls to search their life partner. Scammers were taking advantage of these. They are easily fooling their virtual partner, by assuring them that they are in love with them and planning to settle in the future. After convincing their virtual partner, they begin to gather precious and valuable information regarding banking credentials. Afterward, they scam their virtual partner and easily move out the relation as there is no evidence since the whole thing happens virtually [17].

7) Bitcoin scams: Digital currencies being in electronic format are prone to losses arising out of hacking, loss of passwords, etc. Due to lack of any authorized central agency to regulate the payments or redressal of grievances, scammers are taking advantages of this to fool public and gain their money [18].

TABLE I. NO OF PUBLICATIONS IN LAST TEN YEARS [19]

Year → Attacks↓	2020	2019	2018	2017	2016	2015	2014	2013	2012	2011
Phishing Attack	64	468	844	397	329	351	617	266	270	206
Nigerian Scams	24	249	546	249	323	267	404	994	329	197
Greeting Card Scams	15	84	390	139	167	180	687	302	101	74
Credit Card/Bank Loan Scam	54	346	603	421	463	348	1409	819	430	215
Hitman Scams	1	38	10	12	7	10	11	12	11	5
Online Romance Scams	17	165	208	236	247	196	486	184	135	84
Bitcoin Scams	60	461	714	217	137	102	67	22	8	1

Table I depicts the last ten years' publication report of various banking attacks as mentioned above. It is clear from the above table that the maximum number of researchers are researching on attacks like phishing scams, credit/debit card scams followed by greeting card scams. Bitcoin scams or cryptocurrency scams are an example of the latest type of scam.

B. Statewise of Online fraud cases reported are as follows:

State-wise M-Banking fraud case reports are shown in the graph below. Fig. 1. depicts that Maharashtra [20] had the maximum number of fraud cases reported followed by Delhi, Tamil Nadu, Bihar, Haryana, and Uttar Pradesh. Therefore it is clear although the world is shifting toward digitization, it is not completely secure. To avail the benefit of digitization, it has now become mandatory to gain knowledge regarding cyber-crime and cybersecurity too.

C. Bankwise last ten years(2009-2019) registered online fraud cases are as follows:

A bank is the financial pillar of any nation. The public feels secure to keep their money at the bank than at home. The banking industry is moving toward digitization for providing better and quick services to their customer. Digitization has many advantages but it has some disadvantages too. The security issue is one of the main drawbacks of digitization. Banking industries are also facing these issues.

Table II reports illustrated the last ten years of bank fraud cases in India. ICICI bank encounters a maximum number of fraud cases with a loss of 5,033 crores of money followed by State Bank of India (SBI), Housing Development Finance Corporation (HDFC), The Bank of Baroda and so on [21].

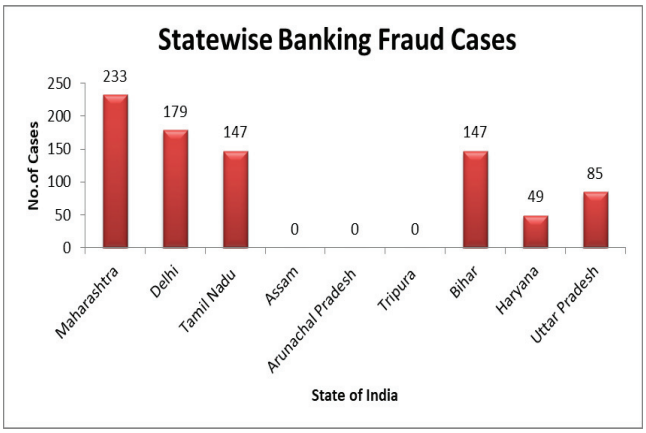

Fig. 1. State wise M-Banking fraud cases registered [20].

TABLE II. BANKS FRAUD CASES REPORT [21]

Bank	No. of Cases	Losses in Crore
ICICI	6,811	₹ 5,033
State Bank of India (SBI)	6,793	₹ 23,734.74
HDFC	2,497	₹ 1,200.79
The Bank of Baroda	2,160	₹ 12,962.96
Punjab National Bank	2,047	₹ 28,700.74
Axis Bank	1,944	₹ 5,301.69
Bank of India	1,872	₹ 12,358.20
Syndicate Bank	1,783	₹ 5,830.85
Central Bank of India's	1, 613	₹ 9,041.98
IDBI Bank Ltd	1,264	₹ 5,978.96
Standard Chartered Bank	1,263	₹ 1,221.41
Canara Bank	1,254	₹ 5,553.38
Union Bank of India	1,244	₹ 11,830.74
Kotak Mahindra	1,213	₹ 430.46
Indian Overseas Bank	1,115	₹ 12,644.70
Oriental Bank of Commerce	1040	₹ 5,598.23
The United Bank of India	944	₹ 3,052.34
State Bank of Mysore	395	₹ 742.31
State Bank of Patiala	386	₹ 1,178.77
Punjab and Sind Bank	276	₹ 1,154.89
UCO Bank	1081	₹ 7,104.77
Tamilnad Mercantile Bank Ltd	261	₹ 493.92
Lakshmi Vilas Bank Ltd	259	₹ 862.64

V. CONCLUSIONS

Some online scams are very well organized and convincing too. The difficult issue is that the people behind these scams are very difficult to identify and catch, that's why this type of scams are increasing daily. To protect ourselves from these types of scams we need to be very alert and aware of the latest types of online fraud strategies. National and private banks play a very crucial role in the economic growth of the nation. Online scams not only affect the individual but also directly or indirectly affecting the nation. Since almost in the daily newspaper we are getting

news regarding online banking fraud cases; therefore it is exceptionally vital growing global issues that need to be addressed on earnest premise.

REFERENCES

[1] Abu-Shanab, E., & Matalqa, S. "Security and Fraud Issues of E-banking". International Journal of Computer Networks and Applications, 2(4), 179-188, 2015.

[2] Sharma, S., & Gaherwal, R. "Comparative Study and Analysis of Unique Identification Number and Social Security Number". Int. Journal of Scientific Research in Computer Science and Engineering, 27, 2017.

[3] John, S. N., Anele, C., Kennedy, O. O., Olajide, F., & Kennedy, C. G. "Realtime fraud detection in the banking sector using data mining techniques/algorithm". In 2016 international conference on computational science and computational intelligence (CSCI) (pp. 1186-1191). IEEE, 2016.

[4] Yazdanifard, R., WanYusoff, W. F., Behora, A. C., & Sade, A. B. "Electronic banking fraud: The need to enhance security and customer trust in online banking". Advances in Information Sciences and Service Sciences, 3(10), 505-509, 2011.

[5] Rohan Abraham, "No TitIndian banks lost Rs 109.75 crore to theft and online fraud in FY18le," Moneycontrol, 2019. [Online]. Available: https://www.moneycontrol.com/news/trends/current-affairs-trends/indian-banks-lost-rs-109-75-crore-to-theft-and-online-fraud-in-fy18-2881431.html. [Accessed: 22-Dec-2019].

[6] Modi, K., & Dayma, R. "Review on fraud detection methods in credit card transactions". In 2017 International Conference on Intelligent Computing and Control (I2C2) (pp. 1-5). IEEE, 2017.

[7] Bhasin, M. L. "An empirical study of frauds in the banks". European Journal of Business and Social Sciences, 4(07), 2015.

[8] Deshwal, P. "A study of mobile banking in India". International Journal of Advanced Research in IT and Engineering, 4(12), 1-12, 2015.

[9] Mhamane, S. S., & Lobo, L. M. R. J. "Internet banking fraud detection using HMM". In 2012 Third International Conference on Computing, Communication and Networking Technologies (ICCCNT'12) (pp. 1-4). IEEE, 2012.

[10] Von Solms, R., & Van Niekerk, J. "From information security to cyber security". Computers & Security, 38, 97-102, 2013.

[11] Aggelis, V. "Offline Internet banking fraud detection". In First International Conference on Availability, Reliability and Security (ARES'06) (pp. 2-pp). IEEE, 2006.

[12] Hong, J. "The state of phishing attacks". Communications of the ACM, 55(1), 74-81, 2012.

[13] Park, Y., Jones, J., McCoy, D., Shi, E., & Jakobsson, M. Scambaiter: Understanding targeted nigerian scams on craigslist. system, 1, 2, 2014.

[14] Minnaar, A. "'You've received a greeting e-card from...': the changing face of cybercrime e-mail spam scams". Acta Criminologica: African Journal of Criminology & Victimology, 2008(Special Edition 2), 92-116, 2008.

[15] Upadhyay, D. "Banking Scams in India". Journal of Banking and Insurance Law, 1(2), 7-13, 2019.

[16] National White Collar Crime Ctr, United States of America, US Federal Bureau of Investigation, Office for Victim Assistance, & United States of America. (2010). Internet Crime Report 2009.

[17] Whitty, M. T., & Buchanan, T. (2012). The online romance scam: A serious cybercrime. CyberPsychology, Behavior, and Social Networking, 15(3), 181-183.

[18] Dumitrescu, G. C."Bitcoin–a brief analysis of the advantages and disadvantages". Global Economic Observer, 5(2), 63-71, 2017. (2020). [https://dimensions.ai.].

[19] BS Web Team, "Maharashtra tops in ATM frauds, Delhi, Tamil Nadu, Karnataka follow," Business Standard, 2019. [Online]. Available: https://www.business-standard.com/article/finance/maharashtra-tops-in-atm-frauds-delhi-tamil-nadu-karnataka-follow-119072200187_1.html. [Accessed: 22-Dec-2019

[20] Livemint, "Bank frauds worth □2.05 trillion happened in last 11 years, reveals RBI data," Livemint, 2019. [Online]. Available: https://www.livemint.com/industry/banking/bank-frauds-worth-rs-2-05-trillion-happened-in-last-11-years-reveals-rbi-data-1560335835680.html. [Accessed: 22-Dec-2019]

[21] How software size influence productivity and project durationInternational Journal of Electrical and Computer Engineering

[22] S. Ghosh, A. Rana, V. Kansal, "A statistical comparison for evaluating the effectiveness of linear and nonlinear manifold detection techniques for software defect prediction" in International Journal of Advanced Intelligence Paradigms , Vol. 12, pp 370-391 (2019).

[23] M. S. Meena, P. Singh, A. Rana, D. Mery, M. Prasad, "A Robust Face Recognition System for One Sample Problem", in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), pp 13-26 (2019).

[24] B. N .Pandey, A. K. Shrivastava, A. Rana, " A Literature Survey of Optimization Techniques for Satellite Image Segmentation", in International Conference on Advanced Computation and Telecommunication, ICACAT 2018 (2018).

[25] P. Navaney, G. Dubey, A. Rana, "SMS Spam Filtering Using Supervised Machine Learning Algorithms", in Proceedings of the 8th International Conference Confluence 2018 on Cloud Computing, Data Science and Engineering, Confluence 2018, pp 43-48 (2018).

[26] H. Walia, A. Rana, V. Kansal, "A Supervised Approach on Gurmukhi Word Sense Disambiguation Using K-NN Method" in Proceedings of the 8th International Conference Confluence 2018 on Cloud Computing, Data Science and Engineering, Confluence 2018, pp 743-746 (2018).

[27] S. Ghosh, A. Rana, V. Kansal, "A Hybrid Nonlinear Manifold Detection Approach for Software Defect Prediction" in 7th International Conference on Reliability, Infocom Technologies and Optimization: Trends and Future Directions, ICRITO 2018, pp 453-459 (2018).