

An Overview of Cyber Security in Digital Banking Sector

S. Chandra Sekhar^{1*}, Manojkumar Kumar²
Sree Vaidyanathan Institute of Management
Corresponding Author: S Chandra Sekhar
chandrasedkhar.s@vidyanikethan.edu

ARTICLE INFO

Keywords: Cyber Attacks,
Cyber Security, Digital
Banking

Received : 07 November
Revised : 09 December
Accepted: 11 January

©2022 Sekhar : This is an open-access
article distributed under the terms of
the [Creative Commons Attribution 4.0
International](https://creativecommons.org/licenses/by/4.0/).



ABSTRACT

In the 21st century the online technology as updated with high performance and used widely by all users. In top five the Digital Banking Sector is also one which makes use of online technology constantly such as NEFT, Googlepay, Phonepe etc. Though there are more usage of Online banking but still the cybercrime in the banking sector has been increasing over the years. As reported 50% of cybercrime is happened related to ATM, debit card and net banking. Banking sector is facing cyber attacks more times compared to other sectors. This paper view the cyber attacks in the banking sector and way of providing the cyber security to those attacks.

INTRODUCTION

Cyber threats are attempts to destroy data in a computer network/system. These cyber threats are originated from various sources like websites or computer system. The main task of Cyber threats to target to an attempt to obtain sensitive information through online channels from many sectors. In many sectors the Digital Banking is affected by Cyber threats in more number. A cyber threat is any malicious act that attempts to gain access to a Digital Banking without authorization or permission from the Account holder. Where a security breach or customers of a major bank having money stolen from their accounts. In the year 2021, banks from all over the world have been hit by hackers. The main aim of cyber Security in Digital Banking is to provide safety measures to the user's account digital money like debit cards and credit cards for transactions.

THEORETICAL REVIEW

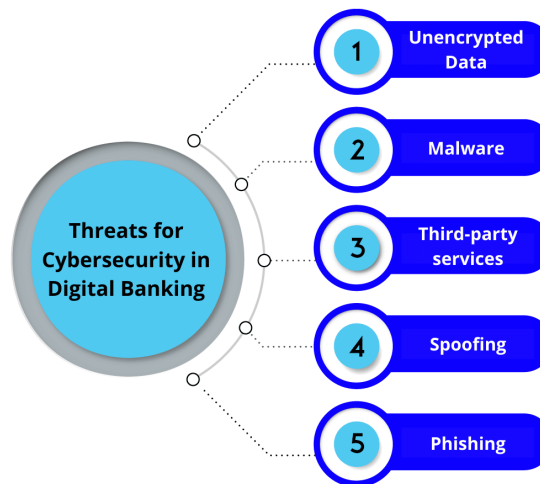


Figure 1. Threats for Cyber security in Digital Banking

1. Unencrypted Data

It is a common threats faced in all digital banking where the data is left unencrypted(Unhidden), and those data was easily used by hackers or cybercriminals thereby creating severe issues in the digital banking.

2. Malware

Peer- to - Peer user devices does digital transaction hence it must be secured. This malware software does serious attacks in the digital banking by hacking the sensitive data which is passed through the network.

3. Third Party Services

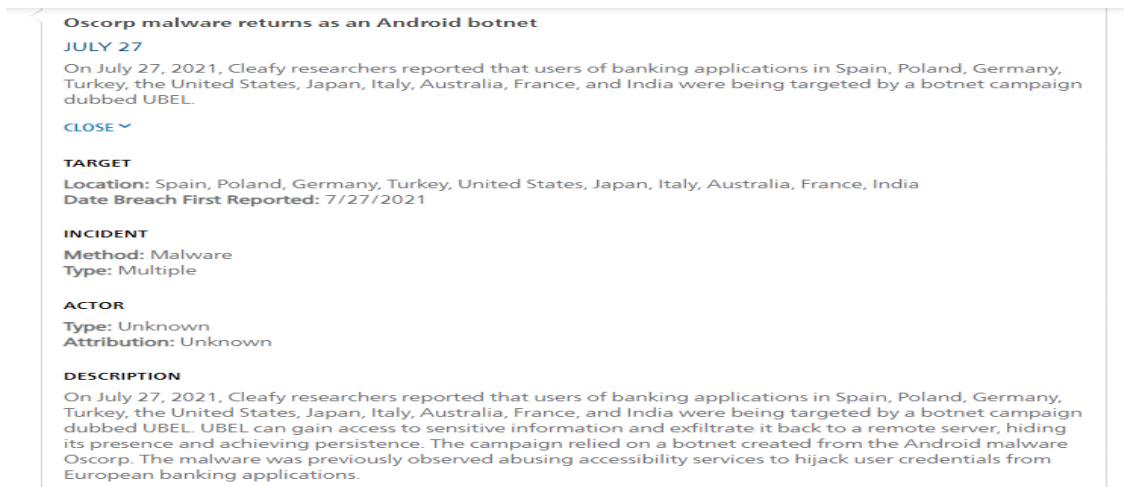
Many banks and financial institutions use third-party services to serve their bank holders better. If the user shares their bank details such as ATM pin, CVV, OTP to third party then there will be hacking of bank details.

4. Spoofing

It is the newest forms of cyber threats faced by digital banking. The cybercriminals will simulate the Banking website's URL which looks like the original Website and even functioning too. When any user enters his or her login Window that time the Bank details are stolen by criminals and use it later.

5. Phishing

It is the oldest and most popular cyber threats where it attempts to get sensitive information such as ATM PIN, CVV, OTP , Credit card/ debit card details etc through Email/ Phone call or SMS.



The image shows a security alert interface. At the top, it says "Oscorp malware returns as an Android botnet" with a date of "JULY 27". The main text reads: "On July 27, 2021, Cleafy researchers reported that users of banking applications in Spain, Poland, Germany, Turkey, the United States, Japan, Italy, Australia, France, and India were being targeted by a botnet campaign dubbed UBEL." Below this is a "CLOSE" button. The "TARGET" section lists "Location: Spain, Poland, Germany, Turkey, United States, Japan, Italy, Australia, France, India" and "Date Breach First Reported: 7/27/2021". The "INCIDENT" section lists "Method: Malware" and "Type: Multiple". The "ACTOR" section lists "Type: Unknown" and "Attribution: Unknown". The "DESCRIPTION" section repeats the main text and adds: "UBEL can gain access to sensitive information and exfiltrate it back to a remote server, hiding its presence and achieving persistence. The campaign relied on a botnet created from the Android malware Oscorp. The malware was previously observed abusing accessibility services to hijack user credentials from European banking applications."

Figure 2. Oscorp Malware Returns as an Android Botnet

METHODOLOGY

Though there are more usage of Online banking but still the cybercrime in the banking sector has been increasing over the years. As reported 50% of cybercrime is happened related to ATM, debit card and net banking. Banking sector is facing cyber attacks more times compared to other sectors. This paper view the cyber attacks in the banking sector and way of providing the cyber security to those attacks. A cyber threat is any malicious act that attempts to gain access to a Digital Banking without authorization or permission from the Account holder. Where a security breach or customers of a major bank having money stolen from their accounts. In the year 2021, banks from all over the world have been hit by hackers. The main aim of cyber Security in Digital Banking is to provide safety measures to the user's account digital money like debit cards and credit cards for transactions.

RESULTS AND DISCUSSIONS

Banking trojan targets Indian Android-based financial customers
SEPTEMBER 22
 On September 22, 2021, researchers reported that Android phone banking customers in India were being targeted the Drinik banking trojan malware.
[CLOSE](#)

TARGET
 Location: India Date Breach First Reported: 9/22/2021

INCIDENT
 Method: Malware
 Type: Multiple

ACTOR
 Type: Unknown
 Attribution: Unknown

DESCRIPTION
 On September 22, 2021, researchers reported that Android phone banking customers in India were being targeted the Drinik banking trojan malware. The malware stole users' personal data and funds using phishing techniques.

Figure 3. Cases of Attack in Cyber Security in Digital Banking India in 2021

Oscorp malware returns as an Android botnet
JULY 27
 On July 27, 2021, Cleafy researchers reported that users of banking applications in Spain, Poland, Germany, Turkey, the United States, Japan, Italy, Australia, France, and India were being targeted by a botnet campaign dubbed UBEL.
[CLOSE](#)

TARGET
 Location: Spain, Poland, Germany, Turkey, United States, Japan, Italy, Australia, France, India
 Date Breach First Reported: 7/27/2021

INCIDENT
 Method: Malware
 Type: Multiple

ACTOR
 Type: Unknown
 Attribution: Unknown

DESCRIPTION
 On July 27, 2021, Cleafy researchers reported that users of banking applications in Spain, Poland, Germany, Turkey, the United States, Japan, Italy, Australia, France, and India were being targeted by a botnet campaign dubbed UBEL. UBEL can gain access to sensitive information and exfiltrate it back to a remote server, hiding its presence and achieving persistence. The campaign relied on a botnet created from the Android malware Oscorp. The malware was previously observed abusing accessibility services to hijack user credentials from European banking applications.

Figure 4. Lack of Cyber Security in E-Banking



Figure 5. Lack of Awareness

1. Lack of Awareness
Most of people have low knowledge about cyber security methods to be implemented in the Digital Banking.
2. Inadequate Budgets and Lack of Management
The Cyber security is accorded low priority, this results to neglect in the budgets as well as Top management focus also remains low on Cyber security.
3. Weak Identity and Access Management
Identity and access management is known as basic element of cyber security but, when the identity and accessing is weak the hackers can easily access the bank account.
4. Rise of Ransomware
It is one of the most important tool. Where a user critical data can be encrypted. So this method can be implemented to all system.
5. Mobile Devices and Apps
Most of the Apps are used for digital banking. Hacker made mobile phones as attractive target to hacks the mobile phone banking transaction. Social Media: Using the social media most of the hackers exploiting in the digital banking.

Cyber Security in E-Banking:

1. Integrated Security
As BFSI [Breath First Search Integrated] is the best technology highly regulated in Digital Banking to integrated security where all components work and communicate together is more beneficial with more security.
2. Encrypted Data
All Banking data that is stored on computers or online must be fully encrypted that means the details of Digital banking should be hidden or unreadable format. Hence those data cannot be stolen or use by the cyber criminals.
3. Machine Learning and Big Data Analytics
A new generation of analytical security where store access a huge number of real time bank data with more security.
4. Understand the Importance of Security
Make the mindset as security as a positive view and go through the risk of security threats and its impact must be analyzed to know the importance of the cyber security.

5. Protect Information

Now a days the data can be stored either in different devices or in the cloud, hence those data will be protected with security.

6. Consumer Awareness

It is one of the important tool where all customers as get the knowledge of securities measures which can be implemented in the Digital Banking.

7. Anti-malware Applications

An anti-malware increase protection, it is the latest application that can potentially defeat the attacks related to digital banking.

CONCLUSIONS AND RECOMMENDATIONS

IT is become the backbone of the Digital banking system. It provides a best support for the digital banking. Presently the digital banking sector where attacks by cyber crimes like, phishing, hacking, forgery, cheating etc. are committed. By ensuring authentication, identification and verification techniques the cyber crimes can be prevented. The weapons for cyber crime is Cyber Security which is used in digital banking as one of the best and important tool. With the growth of digitalization in the banking the threats or attacks from cyber criminals as became more to avoid that the cyber security awareness and different cyber security techniques are used.

In the 21st century the online technology as updated with high performance and used widely by all users. In top five the Digital Banking Sector is also one which makes use of online technology constantly such as NEFT, Googlepay, Phonepe etc. Though there are more usage of Online banking but still the cybercrime in the banking sector has been increasing over the years. As reported 50% of cybercrime is happened related to ATM, debit card and net banking. Banking sector is facing cyber attacks more times compared to other sectors. This paper view the cyber attacks in the banking sector and way of providing the cyber security to those attacks.

Cyber threats are attempts to destroy data in a computer network/system. These cyber threats are originated from various sources like websites or computer system. The main task of Cyber threats to target to an attempt to obtain sensitive information through online channels from may sectors. In many sectors the Digital Banking is affected by Cyber threats in more number. A cyber threat is any malicious act that attempts to gain access to a Digital Banking without authorization or permission from the Account holder. Where a security breach or customers of a major bank having money stolen from their accounts. In the year 2021, banks from all over the world have been hit by hackers. The main aim of cyber Security in Digital Banking is to provide safety measures to the user's account digital money like debit cards and credit cards for transactions.

FURTHER STUDY

Though there are more usage of Online banking but still the cybercrime in the banking sector has been increasing over the years. As reported 50% of cybercrime is happened related to ATM, debit card and net banking. Banking sector is facing cyber attacks more times compared to other sectors. This paper view the cyber attacks in the banking sector and way of providing the cyber security to those attacks. A cyber threat is any malicious act that attempts to gain access to a Digital Banking without authorization or permission from the Account holder. Where a security breach or customers of a major bank having money stolen from their accounts. In the year 2021, banks from all over the world have been hit by hackers. The main aim of cyber Security in Digital Banking is to provide safety measures to the user's account digital money like debit cards and credit cards for transactions.

REFERENCES

- Dr. M. Lokanadha Reddy , Mrs. V. Bhargavi "Cyber security attacks in banking sector: Emerging security challenges and Threats".
- Nandkumar Saravade, Director, "Cyber Security and Compliance NASSCOM : Cyber Security Initiatives in India"
- Claessens, J., Dem, V., De Cock, D., Preneel, B., & Vandewalle, J. (2002). On the security of today s online electronic banking systems. *Computers & Security*, 213: 253-265.
- Agrawal, D. K. (2022). An Empirical Study On Socioeconomic Factors Affecting Producer's Participation In Commodity Markets In India. *Journal of Positive School Psychology*, 2896-2906.
- Basha, M., Singh, A. P., Rafi, M., Rani, M. I., & Sharma, N. M. (2020). Cointegration and Causal relationship between Pharmaceutical sector and Nifty-An empirical Study. *PalArch's Journal of Archaeology of Egypt/Egyptology*, 17(6), 8835-8842.
- Basha, S. M., & Kethan, M. (2022). Covid-19 Pandemic and the Digital Revolution in Academia and Higher Education: an Empirical Study. *Eduvest-Journal of Universal Studies*, 2(8), 1-648.
- Basha, S. M., & Ramaratnam, M. S. (2017). Construction of an Optimal Portfolio Using Sharpe's Single Index Model: A Study on Nifty Midcap 150 Srips. *Indian Journal of Research in Capital Markets*, 4(4), 25-41.
- Basha, S. M., Kethan, M., & Aisha, M. A. A Study on Digital Marketing Tools amongst the Marketing Professionals in Bangalore City.

- DrSanthosh Kumar, V., & Basha, S. M. (2022). A study of Emotional Intelligence and Quality of Life among Doctors in PandemicCovid 19. *International Journal of Early Childhood*, 14(02), 2080-2090.
- Durgaraju, R., & Sekhar, S. C. (2021). A Perspective Research Study on the New Age Currency (The Case of Bit coin Currency System). *International Research Journal of Innovations in Engineering and Technology*, 5(2), 16.
- JagadeeshBabu, M. K., SaurabhSrivastava, S. M., & AditiPriya Singh, M. B. S. (2020). INFLUENCE OF SOCIAL MEDIA MARKETING ON BUYING BEHAVIOR OF MILLENNIAL TOWARDS SMART PHONES IN BANGALORE CITY. *PalArch's Journal of Archaeology of Egypt/Egyptology*, 17(9), 4474-4485.
- Karumuri, V. (2016). Employee engagement: Hotel industry. *SCMS Journal of Indian management*, 13(3), 120-128.
- Karumuri, V. (2016). Employee engagement: Hotel industry. *SCMS Journal of Indian management*, 13(3), 120-128.
- Karumuri, V. (2017). A theoretical framework on employee engagement. *Asia Pacific Journal of Research*, 1, 150-155.
- Kethan, M., & Basha, M. (2022). Relationship of Ethical Sales Behaviour with Customer Loyalty, Trust and Commitment: A Study with Special Reference to Retail Store in Mysore City. *East Asian Journal of Multidisciplinary Research*, 1(7), 1365-1376.
- Kotni, V. V., & Karumuri, V. (2014). An empirical study on the identification of salesforce engagement drivers: A study of selected retail outlets in Visakhapatnam.
- VV DEVI PRASAD KOTNI & VENKATESWARLU K (2014). An Empirical Study on the Identification of Salesforce Engagement Drivers: A Study of Selected Retail Outlets in Visakhapatnam. *Prabandhan: Indian Journal of Management*, 7(7), 31-45.
- Krishnamoorthy, D. N., & Mahabub Basha, S. (2022). An empirical study on construction portfolio with reference to BSE. *Int J Finance Manage Econ*, 5(1), 110-114.
- Kumar, T. S., & Sekhar, S. (2019). Impact of e-Marketing on Influencing Consumer Purchase decision. *International Journal of Scientific Development and Research*, 4(11).

- Kumarai, G. S., Bajaj, P. K., Rana, S. S., Kethan, J., Basha, S. M., & Karumuri, V. (2022). An empirical study on customer satisfaction towards organized Retail outlets in Bengaluru city, Karnataka. *Academy of Marketing Studies Journal*, 24, 1-11.
- Mohammed, B. Z., Kumar, P. M., Thilaga, S., & Basha, M. (2022). An Empirical Study On Customer Experience And Customer Engagement Towards Electric Bikes With Reference To Bangalore City. *Journal of Positive School Psychology*, 4591-4597.
- Nethala, V. J., Pathan, M. F. I., & Sekhar, M. S. C. (2022). A Study on Cooperative Banks in India with Special Reference to Marketing Strategies. *Journal of Contemporary Issues in Business and Government* Vol, 28(04).
- Rajasulochana, D., & Khizerulla, M. (2022). Service Quality In SBI: An Assessment Of Customer Satisfaction On E-Banking Services. *Journal of Positive School Psychology*, 4585-4590.
- Rajasulochana, D., & Murthy, S. (2022). E-Banking And Customers' Satisfaction In Public And Private Sector Banks In Karnataka: An Empirical Analysis. *Journal of Positive School Psychology*, 6(8), 8270-8279.
- Rajesh, D., & Rajasulochana, D. M. (2022). A STUDY ON FACTORS INFLUENCING THE PURCHASE OF ELECTRIC VEHICLES IN INDIAN AUTO MOBILE MARKET. *Journal of Contemporary Issues in Business and Government* Vol, 28(04)
- Rana, S. (2022). Consumer Awareness and Perception Towards Green Marketing: An Empirical Study In Bangalore City. *Journal of Positive School Psychology* <http://journalppw.com>, 6(5), 4240-4245.
- Sekhar, M. S. C., Ashalatha, D., & Gorkhe, M. (2022). Corporate Governance-Impact on Financial Performance of Selected IT Companies in Bengaluru City. *Journal of Contemporary Issues in Business and Government* Vol, 28(03).
- Sekhar, M. S. C., Murthy, J., Karim, S., Reddy, M. M. S., & Bhupathi, C. Factors Influencing Customers' Buying Behaviour: A Study of Electric Vehicles with reference to Tirupati City.
- Sekhar, S. C. (2020). A Study on Effectiveness of Electronic banking System. *Sanshodhan*, 9, 8-13.

- Sekhar, S. C., & Radha, N. (2019). Impact of globalization on msme: prospects, challenges and policy implementation on economic growth. *International Journal of Trend in Scientific Research and Development*, 3(6), 536-541.
- Shaik, M. B., Kethan, M., & Jaggaiah, T. (2022). Financial Literacy and Investment Behaviour of IT Professional With Reference To Bangalore City. *Ilomata International Journal of Management*, 3(3), 353-362.
- Shaik, M. B., Kethan, M., Jaggaiah, T., & Khizerulla, M. (2022). Financial Literacy and Investment Behaviour of IT Professional in India. *East Asian Journal of Multidisciplinary Research*, 1(5), 777-788.
- Shaik, M. B., Kethan, M., Rani, I., Mahesh, U., Harsha, C. S., Navya, M. K., & Sravani, D. (2022). WHICH DETERMINANTS MATTER FOR CAPITAL STRUCTURE? AN EMPIRICAL STUDY ON NBFC'S IN INDIA. *International Journal of Entrepreneurship*, 26, 1-9.
- Venkateswarlu, K., & Prasad, P. V. (2012). A Review on employability skills. *IOSR Journal of Humanities and Social Science*, 2, 32-34.