IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

AN OVERVIEW OF CYBERSECURITY IN BANKING SECTOR

1Dr.L.Mythili, 2KIRUTHIKA. R,

1Associate Professor, 2II MCOM(CA),

1Department of Commerce,

Sri Ramakrishna College of Arts & Science for Women, Coimbatore,India

Abstract: One of the quickest and most simple methods to make payments these days is through the internet. The Internet banking and electronic commerce (E-commerce) sectors face significant challenges due to the potential threat of cyber security incidents. In order to close the gap between banks and clients, we first thoroughly analyze the cyber security of online banking in three developing nations and then suggest a novel strategy to lower the risk associated with cyber security. Because banks are frequently the target of cyber attacks, they have effective security measures in place as well. In addition to analyzing current bank problems, this study suggests a method for identifying and visualizing data leakage risk. This paper's first section compares the most frequent risks to the banking industry based on information from cyber security firms and bank reports. In the end, the authors concluded that insider knowledge—which comes via data leaks—is essential. This study compares and contrasts current bank threats, demonstrating a method for identifying and visualizing the risk of data loss.

Index Terms **- Cyber security, Banking**

I. INTRODUCTION

Cyber security includes all aspects of protecting company assets, people and data from online attacks. As network attacks become more frequent and sophisticated, business networks become more complex, creating a need for network security solutions to reduce risks for network companies. Banks and other financial institutions face new threats to the safety and security of information, an important asset of every company. In the age of the Internet of Things, crimes and information theft have become more complex and sophisticated, and thieves are increasingly using technology to resist arrest. Technology-related barriers in finance. As cybersecurity attacks become less limited, banks need to invest in systems and technologies that can do more than prevent incidents. Protecting customer assets is a clear reason why cybersecurity is critical for the banking industry. Physical credit scanners and online check pages have increased in popularity as more people choose to withdraw cash. Information may be transferred elsewhere and used for criminal purposes.

REVIEW OF LITERATURE:

(Al-alawi, 2020) studied "The Significance of Cyber security System in Helping Managing Riskin Banking and Financial Sector" The goal of this study is to show the major impact and benefits of implementing cyber security in an organization's systems, with an emphasis on the banking sector. In addition, the goal of this research is to promote the use of cyber security in order to keep information safe and properly manage risk. Many banking and financial institutions, on the other hand, remain cautious when it comes to the application and usage of cyber security. In fact, many financial organizations may be completely unaware of the

advantages of cyber security. Furthermore, its application's higher expenditures could be a factor in its rejection. As a result, numerous questions were posed to measure the level of cyber security awareness and abilities in these banks.

According to a 2018 study by Alghazo, Kazmi, and Latif, "Cyber Security Analysis of Internet Banking in Emerging Countries: User and Bank perspectives" Internet banking is commonly promoted as a convenient banking option. It is also referred to as Electronic banking (E-banking), Online banking, and Virtual banking. alternative, in line with the research. In the banking industry, online banking has shown to be a successful and ideal banking option.
The study "CYBER SECURITY" was conducted by (Baur-Yazbeck, Frickenstein, & Medine, 2019). According to research, there is a great deal of promise for digital financial services (DFS) to facilitate the inclusion of money and thereby enhance people's lives. However, cybercrime has become a significant concern in the global shift toward more equal financial sectors, affecting the financial markets of developing and rising nations. Authorities in the financial industry, FSPs, and their clients.

The study "Online Banking: Information Security vs. Hackers Research Paper" was conducted by Marshall (2010). Financial institutions include banks and savings and loans, and while both are charged with managing their clients' funds, financial institutions have greater accountability for handling their clients' personal and historical data. Daily transactions include balance amounts, social security payments, withdrawals, and deposits.
(Rajendran, 2018) explored " bank cyber security" I learned about the concept of "Cybercrime as a Service" Given how much technology is used in banking today, it should come as no surprise that customers are frequently just as tech-savvy as or maybe even better than the average bank employee. Banks are no longer able to respond to consumer concerns about remittances, statements, or Account Views with the normal routine comment or tired platitude that "it's a computer problem," "a software issue," or "a technological failure." Customer is undoubtedly aware of the circumstances.

PROTECT YOURSELF FROM CYBER-ATTACKS BY USING SECURE SOFTWARE:

SECURITY AUDIT: A detailed audit is necessary prior to the implementation of any new cyber security software. The research reveals the benefits and shortcomings of the existing configuration. It also produces suggestions that will enable you to make the best investments and help you save money.
FIREWALLS: Cyber security banking is not limited to merely software. To prevent crimes, the right hardware is also required. Using an upgraded firewall, banks can stop criminal activity before it affects other areas of the network.
BIOMETRICS: Compared to a texted code, biometrics is a more secure form of MFA. This kind of authentication uses face recognition, thumbprints, or retina scans to verify a user's identity. It is now more difficult to hack this type of authentication, even if it has been done in the past.
MULTI-FACTOR AUTHENTICATION (MFA): This security feature is essential for users who use web or mobile apps for their banking. A lot of users don't regularly change their passwords. If they do, they just make small changes. MFA reduces by seeking an extra layer of security, you may prevent criminals from accessing the network. A customer's cell phone might receive a six-digit code, for instance.
VIRUSES: Viruses Every time an end-user device connects to your network, including PCs and smartphones, that is infected with a virus, the bank's cyber security is at danger. This connection transfers private data, and if malware has been placed on the end user's device and is not sufficiently protected, it could be able to access the networks of your bank.

EXTRA RISKS ASSOCIATED WITH MOBILE APPS:

The examples shown above merely touch the surface of possible cyber security problems in the banking industry. Other items to exercise attention with are More Dangers Associated with Mobile Apps More consumers are accessing their banks using mobile apps.Knowing how few or no security many of these people have, the likelihood of a crime is significantly increased. At the endpoint, banking software solutions are required to prevent unauthorized activity.

BREACH AT A THIRD-PARTY COMPANY:

As banks' cyber security has improved, hackers have turned to shared banking systems and third-party networks to get access. Criminals won't have much issue breaking in if these aren't as well-protected as the bank.

A HIGHER RISK OF CRYPTOCURRENCY CYBERATTACKS:

Hacks have increased in the emerging world of cryptocurrencies in addition to traditional finance. Due to the banking industry's uncertainty regarding the proper application of cyber security technologies in a constantly evolving environment, attackers have an increased likelihood of stealing large quantities of cash. Particularly when the figure fluctuates rapidly.

THE CURRENNT SITUATION OF BANK CYBERSECURITY :

Indian banks reported 248 successful hacker and criminal data breaches between June 2018 and March 2022; on August 2, 2022, the government alerted Parliament.
11,60,000 cyber attacks were recorded in 2022, according to the Indian government. Three times as much as it was in 2019, according to estimates. India has been targeted of significant cyber attacks, like the phishing effort against the Union Bank of India in 2016 that nearly contributed to a fraudulent transaction of $171 million. Banks are required to enhance their IT risk governance framework; part of this requires the Chief Information Security Officer to take the lead in addition to the Board and the Board's IT committee taking the lead in ensuring that the relevant standards are followed.

REASONS WHY CYBERSECURITY IS IMPORTANT IN BANKING:

Everyone appears to be using digital payment methods like debit and credit cards and to be completely cashless. In this situation, it is crucial to make sure that the necessary cyber security measures are in place to secure your data and privacy. It could be challenging to trust financial institutions following data breaches. That poses a serious problem for banks. A substandard cyber security solution's data breaches might easily force their customer base to leave their firm. When data from a bank is compromised, you usually lose both money and time. Recovering from the same can be difficult and take a while. That would mean checking statements, canceling cards, and keeping an eye out for problems.

TOP CYBERSECURITY THREATS FACED BY BANKS:

Phishing Attacks:

Phishing attacks are among the most common cybersecurity issues facing the financial industry. They can be utilized to breach the network of a financial institution and launch a more potent assault similar to an APT, which could be disastrous for those establishments (Advanced Persistent Threat). APTs let unauthorized users to get access to the system and operate it covertly for extended periods of time. Significant losses in terms of money, data, and reputation could arise from this. Phishing attacks against financial institutions soared in the first quarter of 2021, according to the survey.

TROJANS:

A number of risky strategies that hackers employ to trick their way into safe data are referred to as "Trojan" attacks. Before being loaded onto a PC, a Banker Trojan appears to be reliable software. Nevertheless, it is a virus that is designed to gain access to personal information handled or stored by online banking systems. This type of software contains a backdoor that allows external access to a machine.

APPLICATIONS OF CYBERSECURITY IN BANKING:

1. **Security Monitoring for Networks:**

The process of continuously scanning a network for indications of suspicious or unwanted activity is called network monitoring. It is commonly used in conjunction with firewalls, antivirus programs, and intrusion detection systems (IDS) as security solutions. Network security monitoring can be done automatically or manually with the software.

2. **Software Security:**

Applications that are crucial for business operations are protected by application security. It can assist you in coordinating your security rules with file-sharing rights and multi-factor authentication. It includes features such as an application that permits listing and code signing. Software security is bound to improve with the application of AI in cybersecurity.

3. **Risk Management:**

Risk management, data integrity, security awareness training, and risk analysis are all included in financial cybersecurity. Evaluation of risks and the mitigation of potential harm are fundamental components of risk management. Sensitive data security is another aspect of data security.

CONCLUSION:

The complex subject of cyber security requires expertise in a wide range of disciplines, including but not restricted to computer science and information technology, psychology, economics, organizational behavior, political science, engineering, sociology, and decision sciences.International affairs as well as legislation. While technology measures are important, policy analysts and others may easily become engrossed in the technical details, the truth is that cyber security is not simply a technological issue. Moreover, cross-disciplinary benefits are limited because the majority of cyber security knowledge is segmented along disciplinary boundaries. Some of these connections will be clarified by this primer. Above all, it aims to leave the reader with two basic ideas. The internetThere will never be a fully solved security issue. The answers to the problem are at least as much nontechnical as they are technical, despite their potential limitations in breadth and durability.

REFERENCE:

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.

Dr. M. Lokanadha Reddy , Mrs. V. Bhargavi "Cyber security attacks in banking sector: Emerging security challenges and ThreatsDr. M. Lokanadha Reddy , Mrs. V. Bhargavi "Cyber security attacks in banking sector: Emerging security challenges and Threats.

Sekhar, S. C. (2020). A Study on Effectiveness of Electronic banking system sanshodhan,9 8-13.

Rajendran, V. (2018). Security in Banks. The Journal of Indian Institute of Banking and Finance, 89(01), 26–32.

Al-alawi, P. A. I. (2020). The Significance of Cybersecurity System in Helping Managing Risk in Banking and Financial Sector. Journal of Xidian University,
14(7).https://doi.org/10.37896/jxu14.7/174