WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Cybersecurity in Banking

Mansi Bhatkande, * Jidnyasa Patil, * Mr. Sachin Desai

(Department master of computer applications VTU/KLS Gogte Institute of Technology Belagavi Email: 2gi22mc041@students.git.edu)
(Department master of computer applications VTU/KLS Gogte Institute of Technology Belagavi Email: 2gi22mc62@students.git.edu)
(Department master of computer applications VTU/KLS Gogte Institute of Technology Belagavi Email: smdesai@git.edu)

ABSTRACT:-

We live in a time when information security has become a big problem. Cyber services are the most enjoyable and time saving part of life. On the other hand, people store their data in the cloud, which is processed by cyber. In this case, cyber security is very important. This is an open security problem because many intruders can attack data and hack user information through the server. When we look around, we see many cases related to cybercrime. The security of cloud-based databases has become a major concern. Our research covers information security, including intrusion detection, which can happen anywhere on the planet. Protecting data from intruders has become critical, and intrusion detection should be an important key to detection. How do we know who is stealing data protected by biometrics, fingerprints, passwords, OTPs and other methods if we don't know who the intruder is? Intruder detection has become increasingly important, especially for moving targets such as aircraft and ships. We can only find a solution if we understand the problem. To avoid this, we use machine learning, biometric identification, data learning and hybrid methods. These are system handles that help protect data from intruders by using the best optimization techniques to get accurate data. We presented a model of a banking system where all bank customer transactions are enabled with the help of biometric copies and digital signatures. This proposal suggests the security of the Smart Online Banking System (SOBS) by adding biometric prints, thus reducing the number of threats from an attacker. (1)

The rapid development of the information process of modern society required cyber security in all areas of human activity, because the intentional or unintentional influence of the information sphere from both external and internal sources can damage security and lead to moral, material, financial reputation and other damages.

Cognitive models were developed to determine the protection level of the information network, information security system and critical infrastructure (banks). Scenarios have been developed that reflect the response of the system to a complex maximum weakening of the effects of the main cyber threats. In summary, the practical application of the method provides an opportunity to predict the cyber security situation of banks and promote the implementation of the necessary mechanisms to prevent, protect and control access at the corresponding levels of the network infrastructure.

1. Introduction :-

This research is primarily limited by time constraints. Additional time would allow for a more in-depth study of the study. In

addition, the limited amount of research in this area has limited the amount of information available for cyber security. Additionally, this study was limited by the amount of survey feedback. This study consists of five parts. This introduction is followed by a review of related literature, methodology in the third section, results and discussion in the fourth section, and finally recommendations and conclusion in the fifth section.

Digital transformation in the banking industry can be seen as a great opportunity, but it also brings with it many challenges. Mobile banking and online banking are easy ways to conduct multiple financial transactions during the digital transformation of banking. Customers benefit from such services, but the threat and possibility of cyber-attacks is also a major challenge for these digital services. Cyber attacks, bank fraud, hacking, phishing and security awareness are major challenges of the digital transformation of the banking industry. Overall, customers' awareness of cyber security could be more questionable in many ways. They need to know how to use technology safely when using banks' digital platforms. Customers are often victims of cyber attacks, phishing and hacking, resulting in digital/cyber literacy among banking customers. A major challenge for the banking sector is the development and innovation of digital technology. This was considered an opportunity for growth and development in the bank's current business model and a threat to the sustainability of the bank's business operations.

Information technology also plays an important role in such digital transformation. It provides operational support in various technical aspects and provides a platform for significant innovations in digital services . A serious debate is needed about banking cyber security oversight. As part of digital transformation, banks are now digitizing all banking services, including confidential customer information that is stored and moved over the network. These services are subject to several cyber attacks as mobile phone and internet banking users are less aware. Banks need to strengthen their cyber security policies to protect themselves from such attacks and increase customer satisfaction. Active awareness of ATM roaming among bank customers is also

necessary so that they can protect themselves against such frauds. The widespread problem of skipping an ATM requires targeted action. This is called ATM bypassing when the ATMs are equipped with receiving devices such as rain covers and fake keyboards. Card secrecy is a major factor in the already widespread problem of card fraud in the financial sector.

Cyber security awareness has become a critical parameter to secure our mobile banking applications and online banking operations in the digital transformation of banking. The study covers three major types of cyber security such as cyber attacks, hacking and phishing. To protect against cyber attacks, it is important to study and understand the cyber security awareness of users of mobile banking applications and online banking. This study helps clients understand various general and technical aspects of their cyber security. It also helps banks to understand current customer satisfaction with bank security, cyber security assistance provided by the bank and expectations of cyber security technology supports.

2. Literature review:-

A number of studies have been conducted to identify the importance of cyber security, adoption of digital change and digital transformation in the financial sector, especially in the banking sector. According to a previous study, traditional banks are exposed to cyber attacks when working with fintech companies [4, 5]. Skinner [6] illustrated the impact of social networks on digitization in various industries. The study also explored how digital disruption affects traditional social interactions. The increasing use of mobile devices is another important factor that has benefited the digital transformation process. According to Bain and Company's 22-country survey of digital customers, the use of mobile banking applications grew by 19 percentage points between 2013 and 2014, while the use of desktop banking services remained almost flat [7].

The term "digitalization" was originally coined in 2000 and has since become an important driver of digital transformation, enabling a wide range of business models and organizations [8]. Activities that can harm the organization's assets are classified as threats. Cyber attacks mainly destroy software, hardware and data. Microsoft has created a standard threat classification system called STRIDE..Stolterman and Fors [10] describe digital transformation as "changes caused by digital technology or affecting all aspects of human life". Digitization was originally described as converting text and images into binary numbers. It allows data to be managed, copied and shared cheaply in large volumes and at an affordable price [11]. Digital systems and platforms are evolving, leading to new products, services, business models and behaviors, as well as new ways of working and more efficient ways of developing business processes, all of which affect society [11]. Customer satisfaction, experience, awareness and expectations are all factors to consider when evaluating recent developments in digital transformation.

Mbama and Ezepue believe that a positive customer experience is linked to greater customer satisfaction and loyalty. Customers' experiences with digital banking are influenced by several factors, such as the quality of their contact with staff, service quality, perceived usability, perceived risk and perceived value.

3. Importance of Cyber Security:

1. Everyone seems to be unhappy using digital currency, debit and credit cards.In this context, it has become very important to protect data and privacyto ensure that allcyber security measures are in place.
2. Security breaches can make it difficult to trust financial institutions and banks, this is a serious problem. A weak cyber security systemcan lead to data breaches,which can easily cause the customer base to movetheir money elsewhere.
3. In the event of a data breach, time and money are lost. Compensating damages withcan be time consuming,and stressful. This would require cancelingcards, checking bank statements and flagging problems.
4. Private information in some unacceptable hands can cause enormous damage. Although cardsare canceled and fraudis dealt with immediately, the information is sensitive and can reveal a lot of information that can be misused.
5. Banks should be more vigilantthan most other businesses. This is at the expense of the banks keeping private and valuable personal data. This informationwith a bank can be hacked if it is not protected against cybercriminal threats.

3.1 Finding :

The key findings of this paper is the adoption of digital technology in the banking sector has led to a significant increase in digital fraud, especially in the form of online banking fraud. This article emphasizes that these scams have become a global problem and a developed industry, with cybercriminals using sophisticated tools such as phishing attacks, denial-of- service attacks, Trojans, malware infections, identity theft, and computer viruses.

3.2 Research limitations/implications :

This study is based only on a literature review without baseline data or case studies; Therefore, it may miss the first- hand experience and perspectives of banks and cybersecurity professionals

3.3 Practical implications :

This study highlights the need for banks to implement enhanced security measures to secure their online banking systems.

3.4 Social Implications

This study emphasizes the importance of ongoing training and awareness programs for both bank employees and customers..

3.5 Originality/value :

This study specifically looks at the adoption of digital technology in the banking sector and its relationship with the growth of digital fraud. This focus on the intersection of technology and fraud in the banking industry is a distinctive aspect. This study conducts a surveillance camera that examines the current techniques used by banks to secure their online banking systems. This comprehensive approach provides an overview of the various security measures that banks use to protect against various cyber threats. of.

4. Common Trends and Differences in Cybersecurity Regulations:

One important trend in cybersecurity regulations is the convergence of global cybersecurity standards. Countries andregions are increasingly aligning their cybersecurity frameworks with internationally recognized standards such as ISO/IEC 27001. This approach aims to create a common basis for cybersecurity practices and facilitatecross-border cooperation in combating cyber threats. Despite efforts to harmonize cybersecurity standards, there are still significant differences in data protection andbreach reporting requirements. For example, the EU's General Data Protection Regulation (GDPR) imposes strictdata protection requirements and data breach notification requirements, including mandatory notification of data breachesto supervisory authorities within 72 hours. In contrast, data protection laws in other jurisdictions may not havesuch strict requirements, leading to differences in cybersecurity practices between jurisdictions. One of the most important challenges in achieving compliance with cybersecurity requirements is the rapidly evolving nature of cyber threats and the corresponding need to update cybersecurity measures accordingly. Financial institutions must constantly monitorand evaluate their cyber security practices to ensure compliance with changing regulations and emerging threats In addition, the complexity of global cybersecurity regulations can present challenges for financial institutions operating in multiple jurisdictions as they mustnavigate different legal requirements and compliance frameworks. Overall, while trends in global cybersecurity standards are converging, there are still significant differences in data protection and breach reporting requirements. Financial institutions must remain vigilant in monitoring regulatory developments and adapting their cyber security practices to ensure they are compliant with evolving regulations and protect against cyber threats. In addition to the convergence of global cyber security standards and differences in data protection and data breach reporting requirements, financial institutions' cyber security regulations share several

4.1 Other common trends and differences:

Many cyber security regulations, such as the US National Standards Institute and the Cyber security Framework of Technology (NIST) and the Monetary Authority of Singapore (MAS) Technology Risk Management Guidelines, emphasize a risk-based approach to cybersecurity . There are differences in regulatory oversight and enforcement mechanisms across jurisdictions. Some regulators, such as the Financial Conduct Authority (FCA) in the UK and the MAS in Singapore, have established specific cyber security guidelines and frameworks for financial institutions and strong monitoring mechanisms for non-compliance. Other jurisdictions, on the other hand, may have less stringent regulations or may rely more on industry self-regulation.

Data protection regulations such as the EU GDPR and the US California Consumer Privacy Act (CCPA) restrict the transfer of personal data outside the jurisdiction.

Financial institutions operating in multiple jurisdictions must comply with these regulations and take measures to ensure the secure transfer of data across borders. Some jurisdictions haveindustry-specific cybersecurity regulations that apply to financial institutions.

Leach-Bliley Act (GLBA) requires financial institutions to implement safeguards to protect customer information. Similarly, the Payment Card Data Security Standard (PCI DSS) sets requirements for organizations that process credit card data.Regulations will address new technologies such as cloud computing, artificial intelligence and blockchain. Financial institutions must consider how these technologies will affect their cyber security practices and ensurecompliance with relevant regulations. Overall, while there are common trends towards risk-based approaches and regulatory oversight, there are also significant differences between jurisdictions in terms of privacy requirements, enforcement mechanisms and sector-specific regulations. Financial institutions must be aware of these differences and adapt their cybersecurity practices to meet the applicable regulations in each jurisdiction in which they operate.

security assessments and employee training. They must also regularly update their security policies and proceduresto address new threats. Financial institutions should work with other institutions, regulators and cyber security organizations to share threat intelligence and best practices. This can help them stay ahead of cyber threats and improve their overall cyber security posture. Financial institutions should prioritize investments in cyber security and allocate sufficient resources to protect their systems and data. They should also be abreast of the latest cyber threats and adjust their security measures accordingly. Financial institutions should adopt a risk-based approach to cybersecurity and focus their efforts on mitigating the most significant business risks. This includes identifying and prioritizing cyber security risks, implementing controls to mitigate those risks and regularly reviewing and updating risk assessments. Financial institutions must ensure compliance with relevant cybersecurity regulations and standards such as GDPR, GLBA, PCI DSS and other applicable standards in their jurisdiction. They should also regularly review their cybersecurity policies to ensure compliance and address any gaps. Financial institutions should use secure technologies such asencryption, secure authentication mechanisms and secure coding practices to protect their systems and data from cyber threats. They must also regularly update their software and systems to address known vulnerabilities. Financial institutions should provide regular cyber security training for their employees to increase awareness of cyber threats and best practicesto protect against them. Employees should be trained to recognize phishing messages, use strong passwords, andreport security information immediately. By following these best practices, financial institutions can improve their cyber security and better protect against cyber threats.

Financial institutions should promote a culture of cyber security awareness and responsibility among all employees. Thisincludes promoting a proactive approach to security, encouraging employees to report suspicious activity andensuring that cyber security is a priority at all levels of the organization. Financial institutions should conduct regular security assessments,including penetration and vulnerability tests, to identify and mitigate potential security risks. These inspections must be carried out by qualified third parties and should cover all aspects of the facility's \security. Financial institutions must ensure that third-party vendors and partners adhere to strict security standards andpolicies. This includes due diligence, including security assessments and audits, andincorporating security requirements into contracts. Financial institutions should provide employees with regular cyber security training andawareness programs. This should include training on phishing awareness, secure password practices and privacy policies. Financial institutions must continually review and improve their cyber security practices based on emerging threats and industry best practices. This includes regularly updating security policies and procedures and investing in new technologies and tools to improve security. By implementing these best practices, financial institutions can strengthen their cyber security and better protect themselves and their customers from cyber threats.

5. Case Studies and Examples:

One of the biggest credit reporting companies, Equifax, had a significant data breach in 2017 that resulted in the exposure of over 147 million customers' personal. The hack happened as a result of Equifax's systems' known vulnerability not being patched, underscoring the significance of timely software updates and vulnerability management. One of the biggest banks in the country, JPMorgan Chase, was the target of a cyberattack in 2014 that exposed the personal data of 7 million small businesses and over 76 million people. Strong access controls and employee training are essential, as the incident was linked to a group of hackers who obtained access to the bank's systems by using employee credentials that were compromised.Bank of America has put in place a thorough cyber security program that includes planning for incident response, personnel training, and routine security assessments. To detect and respond to cyber threats in real-time, the bank has also invested in cutting-edge security technologies like endpoint detection and response (EDR) and security informationand event management (SIEM) systems. Singapore-based DBS Bank has won praise for taking a proactive stance when it comes to cybersecurity. To find and fix these weaknesses, the bank has set up a specialised cyber security team and frequently performs penetration tests and security audits. In order to exchange threat intelligence and best practices, DBS Bank also works with government and business partners.

Cyber security is not only a technical issue, but also a cultural issue. Financial institutions should promote a cybersecurity-aware culture throughout their organization and focus on promoting cybersecurity awareness and responsibility among employees at all levels. Regular training and awareness programs can help employees identify and respond effectively to cyber threats, reducing the risk of insider threats and human error. Cyber threats are often too complex and far- reaching for individual financial institutions to deal with alone. Collaboration with industry partners such as other financial institutions, cybersecurity providers and industry associations can improve collective cybersecurity resilience. Financial institutions can strengthen their defenses and respond more effectively to cyber threats by sharing threat intelligence, best practices and lessons learned.

6. Challenges and Future Directions:

Financial institutions encounter major obstacles in distributing enough resources to address the growing complexity of their operations are increasingly being implemented by organizations to protect their digital assets. Adhering to various regulations in different regions can require a significant amount of resources.demand significant capital in technology, staff, and education. More over, the swift rate of regulatory change Further more, the challenge of achieving is worsened by the absence of alignment among regulatory frameworks adherence to cyber security regulations. Financial institutions must embrace a risk-focused approach in order to tackle these challenges. Adhering to regulations by focusing resources and efforts on the most important cybersecurity threats to their company. They should utilize automated and technological solutions as well.simplify compliance workflows and lessen the administrative load linked to regulatory reporting.writing down informationFinancial institutions work in a constantly evolving landscape of cyber threats, as attackers become more skilled and determined in their assaults. With the introduction of new attack vectors and vulnerabilities, the advent of new technologies like artificial intelligence and the Internet of Things further complicates the cyber security environment.

Financial institutions need to adopt a continuous improvement culture in order to stay ahead of cyber risks. They need to regularly review their cybersecurity processes, technology, and strategies in order to adjust to new threats. This entails making investments in threat intelligence tools, carrying out frequent penetration tests and security evaluations, and encouraging cooperation between colleagues in the business and cyber security specialists to exchange threat intelligence and best practices.Invest resources in addressing the most important cybersecurity threats that the company is now facing, giving special attention to those that could have the most effects on customer confidence and business operations. Work together to share threat intelligence, best practices, and lessons gained with regulators, cybersecurity professionals, and peers in the industry. Engaging in industry forums and information-sharing programmes can improve the resilience of cybersecurity as a whole and speed up the creation of successful cybersecurity plans. Increase insight into cybersecurity threats and vulnerabilities, expedite compliance procedures, and strengthen incident response capabilities by utilising automation techniques and technological solutions. Financial institutions can reduce the time and resources needed for manual activities by implementing automation, which can improve their ability to identify and address cyber threats.The rapid pace of technological innovation and digitaltransformation in the financial sector presents both opportunities and challenges forcybersecurity compliance.

While technologies such as cloud computing, artificial intelligence and blockchain offer significant gains in efficiency and innovation, they also introduce new cybersecurity risks and challenges. Financial institutions must ensure that their cyber security strategies and compliance programs adapt to the evolvingtechnological environment and include measures to mitigate emerging threats you don't do that .This includes strong security management of new technologies, conducting regular risk assessments and integrating cyber security into the design and development of new digital products and services. As cyber security threats evolve, regulators increasingly focus on enforcement and accountability to ensure that financial institutions take appropriate steps to protect their systems and data.

Financial institutions must therefore prioritize security compliance and risk management and implement strong control and governance frameworks to demonstrate their commitment to cyber security best practices. This includes conducting regular audits and transactions, establishing clear responsibility for cyber security within the organization and ensuring transparency about cyber security incidents to regulators and stakeholders. Addressing these challenges and adopting future cybersecurity guidelines iscritical for financial institutions to effectively manage cyber risk, improve their cybersecurity resilience, and maintain customer and stakeholder trust in an increasingly digital and interconnected world.

7. Conclusion:

In summary, a comparative analysis of global standards and regulations for cybersecurity compliance by financial institutions revealed some important findings and recommendations. The study showed that while is in line with internationally recognized standards and best practices, there are still significant challenges and gaps that need to be addressed. First, the study identifies the need for better regulatory alignment and harmonization to reduce complexity and facilitate compliance by MFIs. Policy makers and regulators are encouraged to work together to harmonize cybersecurity rules and standards across jurisdictions, ensuring consistency and clarity for financial institutions operating globally. Second, the study highlighted the importance of a risk-based approach to cyber security compliance, considering evolving cyber threats and the need for continuous improvement. Financial institutions are encouraged to prioritize cybersecurity risk management and invest in innovative technologies and practices to improve their cyber security resilience. Finally, research highlighted the need for collaboration between policy makers, regulators, and financial institutions to address cyber security gaps, promote cyber security education, and increase cyber security awareness and best practices. In light of these findings, policy makers, regulators, and financial institutions are encouraged to work together to improve financial institutions' cybersecurity compliance. By adopting a collaborative and proactive approach, stakeholders can improve cyber security resilience, protect against cyber threats and maintain trust in the financial system. In the future, the future of cybersecurity compliance for financial institutions will be shaped by technological advances, evolving regulatory requirements, and emerging cyber threats. It is imperative that stakeholders remain vigilant, adaptable and collaborative to meet these challenges to ensure a safe and sustainable financial system in the future.

References :-

1. Cyber Risk Management In Indian Banking Sector Sunil Kumar Educational Administration: Theory and Practice 30 (4), 477-486, 2024
2. Cybersecurity in banking and financial sector: Security analysis of a mobile banking application Biswajit Panja, Dennis Fattaleh, Mark ercado, Adam Robinson, Priyanka Meharia 2013 international conference on collaboration technologies and systems (CTS), 397-403, 2013

3. 3.Evaluation of cyber security threats in banking systems Abdul Qarib Stanikzai, Munam Ali Shah 2021 IEEE Symposium Series on Computational Intelligence (SSCI), 1-4, 2021
4. Cyber Security in Banking Sector.Michael Best, Lachezar Krumov, Ioan C Bacivarov International Journal of Information Security & Cybercrime 8 (2), 2019
5. Utilizing bio metric system for enhancing cyber security in banking sector: a systematic analysis Habib Ullah Khan, Muhammad Zain Malik, Shah Nazir, Faheem KhanIEEE Access, 2023
6. Cyber security threats on digital banking Haitham M Alzoubi, Taher M Ghazal, Mohammad Kamrul Hasan, Asma Alketbi, Rukshanda Kamran, Nidal A Al-Dmour, Shayla Islam 2022 1st International Conference on AI in Cybersecurity (ICAIC), 1-4, 2022
7. Cybersecurity in banking: a global perspective with a focus on Nigerian practices Azeez Olanipekun Hassan, Sarah Kuzankah Ewuga,Computer Science & IT Research Journal 5 (1), 41-59, 2024
8. Cyber security threats, vulnerabilities, and security solutions models in banking Diptiben Ghelani, Tan Kian Hua, Surendra Kumar Reddy Koduru Authorea Preprints, 2022
9. H. M. Alzoubi *et al*., "Cyber Security Threats on Digital Banking," *2022 1st International Conference on AI in Cybersecurity (ICAIC)*, Victoria, TX, USA, 2022
10. Utilizing Bio Metric System for Enhancing Cyber Security in Banking Sector: A Systematic Analysis ,2023
11. .hdfcbank.com. (2021). Retrieved from https://www.hdfcbank.com
12. Amrollahi, M., Dehghantanha, A., & Parizi, R. M. (2020). A survey on application of big data in fin tech banking security and privacy. In Handbook of Big Data Privacy (pp. 319-342). Springer, Cham.
13. REVOLUTIONIZING BANKING SECURITY: INTEGRATING ARTIFICIAL INTELLIGENCE, BLOCKCHAIN, AND BUSINESS INTELLIGENCE FOR ENHANCED CYBERSECURITY