DOI: *10.53739/samvad/2024/v28/173776*
ISSN (Print) : 2249-1880
ISSN (Online) : 2348-5329

SAMVAD: SIBM Pune Research Journal, *Vol XXVIII, 01-06, June 2024*

Enhancing Cyber Defenses in Indian Banking Industry

Saurabh Bhattacharya

Chitkara Business School, Chitkara University, Rajpura – 140401, Punjab, India; saurabhbhattacharya18@gmail.com

Abstract

The banking industry is greatly threatened by cybercrime, which makes it necessary to do a thorough investigation to comprehend its effects and forthcoming developments for cybersecurity. Research highlights the constant evolution of cyber risks and the disastrous effects of cyberattacks on Indian banking systems. The study explores the rise in cybercrime, the difficulties that the financial services industry faces, and the pressing demand for creative approaches to cybersecurity. Following cyber regulations and being up to date with new developments is essential for reducing risks and protecting the banking sector as cyberattacks are becoming more complex. The author suggests new-age technology and methods that can be used to tackle cyberattacks in the banking industry.

Keywords: Artificial Intelligence, Cyberattack, Cybercrime, Cybersecurity, Digital Banking, Machine Learning

1. Introduction to Cybercrime and its Background

Cybersecurity is a complex, multifaceted, and challenging-to-grasp problem area. As the number of people using electronic devices increases, the threat environment is still evolving. Identifying and addressing vulnerabilities is the main goal of traditional cybersecurity methodologies (Malinka *et al.*, 2022). This mindset is necessary, but not enough. Gaining more insight into the features of potential and existing cyberattacks is necessary to make wise preventative decisions that optimize the amount of resources available (Agrafiotis *et al.*, 2018). The goal of this project is to identify themes of usual susceptibility that have not yet been identified (Zwilling *et al.*, 2022; Dwyer *et al.*, 2022). The results of our investigation are reported, and their implications are discussed. We then wrap up and provide recommendations for additional research. Numerous security-based innovation methods have been proposed, but not all of them have been empirically tested in real-world settings. As a result, we don't fully comprehend their applicability or true use, particularly in the context of creating financial solutions. One of the main issues with this style of banking is the variety of dangers to privacy that are there (Berjawi *et al.*, 2023). The banking industry is continuously changing technologically as financial services theoretical frameworks shift. To ascertain the advantages, potential, and disadvantages of existing approaches, this article analyses and investigates security solutions in the context of their applicability in creating a safe online banking infrastructure depending on the recognized assessment standards.

To protect the information, systems for networking and computers, and programs from possible attacks via the internet, certain protocols, strategies, and instruments are referred to as "cyber security" (Khan *et al.*, 2023; Zwilling *et al.*, 2022). Attackers can employ Artificial Intelligence technologies for more sophisticated assaults. Deepfakes are currently in use, and robots are still proliferating.

Professionals are no longer required to commute to operate from one specific location nowadays, the prevalence of working in virtual circumstances has forced security professionals to evaluate the commercial hazards associated with remote work and take steps to stop third parties from breaking into or logging into these working conditions. No matter how many sophisticated technological safeguards businesses implement to stave off cyber threats, the "human element"- that is, personnel skills- deserves more attention since it is the most vulnerable component in this chain (Mijwil *et al.*, 2023). The question regarding safety

compliance concerns involve people and their perceptions, understandings, and decisions about how they react to safety hazards, i.e., if they want to follow recommended security procedures. Although researchers and professionals alike acknowledge that people play a crucial role in attaining protection, they are additionally referred to as the most vulnerable component in the protection network since they frequently disregard safety-recommended procedures. As a result, it is not unexpected that a person's security-related conduct has developed into a crucial concern for organizations and a focal point for study. Industry data show that, despite greater leadership attempts to enhance safety, the main driver of breaches is human behaviour- whether intentional, careless, or unintentional. (Donalds & Osei-Bryson, 2020; Cavelty *et al.*, 2023).

Concentrating on cyber security expertise, perception, and conduct, the study finds that although consumers in countries like Israel, Slovenia, Poland, and Turkey exhibit sufficient awareness of online dangers, they take insufficient precautions (Khan *et al.*, 2023). There is a cross-national and gender-neutral relationship between greater consciousness and cyber education. Though not given data, understanding affects the use of protective methods. It is important to emphasize customized cybersecurity strategies based on geographical disparities since nation-specific variables affect how perceptions, understandings, and actions interact (Zwilling *et al.*, 2022; Khan *et al.*, 2023).

1.1 Using Technology in the Current and Future

The fundamental concept of digital safety and adaptive perception is "frameworks." Any disturbance that impairs digital technologies' ability to function normally is referred to as a cyber-attack. Risks are "weaknesses in a computer system, system safety methods, internal safeguards, or execution that might be leveraged by an undesirable source" that make intentional disturbance of the digital world conceivable. It is difficult to completely eradicate current weaknesses from the technological architecture and to stop fresh ones from emerging (Khan *et al.*, 2023).

2. Cybersecurity Risk and Uncertainty's Ethical Component

All leaders must work towards answering the following: For whom is technological safety appropriate? Which degree of cybersecurity is necessary and desirable? (Cavelty *et al.*, 2023; Dwyer *et al.*, 2022). Sadly, because cyber security is a "cruel issue," these concerns are unable to be resolved by reasoning solely. Absurd issues are difficult to address since there isn't one, workable answer since several parties possess distinct objectives and points of view. It is possible to establish a connection with people and collective networks by emphasizing weakness and unpredictability, and these are fundamental ideas in emergency preparedness, human resilience, and technological safety studies (Dwyer *et al.*, 2022).

2.1 Recognizing Embedded Volatility in Cyberspace

Safety measures for businesses, public spaces, electronic goods, and private businesses are becoming more interested in biometric verification. Companies, individuals, and businesses are increasingly using biometric authentication to safeguard cyberspace from attackers as well as other malicious actors (Khan *et al.*, 2023; Kumar & Om, 2018; Debas *et al.*, 2023).

3. Key Trends and Innovations in the World of Cybercrime

Blockchain innovations are upending the banking sector, for instance, and recent advancements in artificial intelligence and machine learning have altered the environment for businesses concerning revolutionary goods and technologies as well as possibilities for corporate executives to motivate representation as further contributors to organizational techniques and management (Demirkan *et al.*, 2020; Hassani *et al.*, 2018; Hasanova *et al.*, 2019). A key factor in the accuracy of classifiers is feature filtering, and XGBoost is a useful technique for reducing the amount of features and processing time (Berjawi *et al.*, 2023). With Android features for detecting malware, dynamic evaluation is a particularly often utilized method. Among the algorithms in occupancy, the machine learning framework makes up the highest share. The majority of the efficiency measures that are used are accurate. The neural network framework works better than the non-neural network framework (Pan *et al.*, 2020; Hussen *et al.*, 2023; Cherqi *et al.*, 2023). Adversarial methods based on Machine Learning (ML) are being used by hackers to modify algorithms. This allows them to avoid identification by security applications and launch complex assaults on financial platforms.

Ransomware attacks pose an alarming level of danger to banking organizations because they encrypt confidential information and expect a fee to unlock it. Such assaults continue to pose significant hazards to the financial industry in 2023 (Blaze, 2023). Internal risks and theft of information continue despite technological developments. Cybercriminals may launch specific attacks or take advantage of vulnerable insiders to obtain unauthorized possession of private financial data (AAG IT Support, n.d.; Porcedda, 2023; Georgiadou *et al.*, 2022; Bamrara *et al.*, 2013). Hazardous malware known as ransomware locks the data of a target once it is triggered and frequently extends across shared networking storage. Unless the assailants get payment and receive an electronic code that unlocks the contents, the data are protected. hackers to take advantage of old or unfixed software flaws. Whenever they come across a machine with software that is vulnerable to a particular attack, they utilize the flaw to install the ransomware straight inside the machine. Hackers search the web for such machines.

One major problem is the identification of malware from unknown sets. The biggest obstacles in the realm of cybersecurity connected to the internet of massive amounts of information are the identification of malware threats and pirated software. Certain papers proposed a deep learning-based method that combines malware and pirated file detection (Ullah *et al.*, 2019; Pan *et al.*, 2020; Iscan *et al.*, 2023).

Phishing refers to a behaviour of social engineering that employs diverse techniques to coerce the intended victim into divulging private data, including but not to their email address, login, login credentials, and banking details. An intruder then uses this knowledge against their target in a negative way (Alabdan, 2020; Mohammad *et al.*, 2015; Goenka *et al.*, 2023; Safi & Singh, 2023).

Nowadays, people spend a significant amount of their time in online spaces, which include various public services, private platforms, and social networks. These conditions are vital, thus strong security against cyber threats- which might range from data theft to system disruptions—is required (Goenka *et al.*, 2023). A complete framework known as cybersecurity uses manager, administrative, and technological controls to stop abuse or illegal use of information technology platforms. This protects users from possible hazards and breaches, guarantees the smooth functioning of these platforms, and preserves the security of their private information. To prevent assaults, malware, and information theft, cybersecurity methods are examined in this paper, with a particular emphasis on the function of Artificial Intelligence (AI) (Khan *et al.*, 2023). In addition, it offers a succinct synopsis of pertinent research, emphasizing the applications and implications of deep learning and machine learning methods in cybersecurity. The results highlight how important these methods are for strengthening computer systems, anticipating and understanding the actions of malicious software, and blocking unintentional involvement and computer infiltration (Mijwil *et al.*, 2023).

Alarming data demonstrate the extent to which cybercrime remains a menace worldwide:

- The prevalence of these assaults is reflected in the projected 53.35 million US individuals who were impacted by cybercriminals in the initial part of 2022 (AAG IT Support, n.d.).
- According to FBI Internet crime data, at least 422 million people were affected by cybercrime, highlighting the severity of the issue (Palatty, 2022).
- According to predictions, the economic impact of cyberattacks is expected to climb to $8 trillion by 2023 and $10.5 trillion by the year 2025 (Brooks, n.d.).
- Analysts from Synopsys reported that 84% of program libraries have a minimum of one open-source threat (Brooks, n.d.).
- It is expected that cybercrime will affect close to $224 Billion in 2023 (Crane, 2023).
- In India, theft of funds is among the many common cybercrimes, including internet-based banking and UPI among frequently victimized platforms (Hindustan Times, 2023).
- Possible weaknesses in the industry are highlighted by the fact that small enterprises' prioritization of cybersecurity is declining, from 80% in 2022 to 68% in 2023 AAG IT Support, n.d.).
- The banking sector is affected by hacking incidents worldwide, as hackers take advantage of weaknesses to reveal billions of sensitive files (Security Intelligence, 2023).

- Despite the rising threats, 51% of organizations in the financial sector plan to increase cybersecurity spending in response to the growing challenge (Statista, n.d.).

4. Ways Ahead

The authors' discussion has made it clear, there isn't just one method to handle cybersecurity. As dispersed, contentious, and pervasive as cybersecurity is in daily existence, many different professional viewpoints and approaches may be used while working on a crucial issue. Cutting-edge preventative methods and dynamic developments will define banking security in the years to come. Techniques like deep learning and machine learning are among the top techniques used to tackle cybercrime today (Ullah *et al.*, 2019; Khan *et al.*, 2023). AI and ML (Machine Learning) allow data-driven decisions to be made using forecasting techniques, reducing the number of funds needed to minimize risks. AI and ML have the potential to detect new assaults more quickly, make scientific conclusions, and deliver that data to consumer protection systems in the framework of cybersecurity. Though they might be beneficial instruments for cyber-defense, AI and ML can potentially have drawbacks. Hackers may additionally utilize it, even though its uses include improving cyber defense capacity and quickly identifying risk abnormalities. Cybercriminals and competitive countries are presently utilizing AI and MI as instruments to locate and take advantage of weaknesses in security monitoring frameworks. Hackers have been attacking and probing targeted systems with AI and machine learning technologies. At risk are tiny companies, organizations, and particularly medical centres that are unable to manage to make large expenditures in protective cutting-edge security technologies like artificial intelligence. Ransomware-based blackmail by attackers requesting cryptocurrency payments may develop into an increasingly enduring and dynamic menace. The proliferation of the World Wide Web of Devices will provide a plethora of fresh opportunities for malicious actors to prey on. To defend towards assaults, governments and the private sector alike must quickly grasp the consequences of the newly developing, evolving information security technologies, such as AI and ML.

5. Conclusion

To identify dangers in transactions that are suspicious, automatic and reliable identification is necessary. The capacity to prevent and detect scams depends on a trustworthy and effective monitoring method as the number of banking scams is frighteningly rising. A rising trend in combating fraud is the use of AI and ML (Mijwil *et al.*, 2023; Ullah *et al.*, 2019) to improve cybersecurity through connected, intelligent gadgets. Strong precautions preventing card cloning are needed, as the financial industry is facing an increase in identity theft and credit card fraud cases. The growth of cybersecurity trends is driven by ongoing technical advancements, necessitating a corresponding expansion in defense methods. Responsive security solutions are necessary for light of the growing threat landscape in cybersecurity, which includes phishing and social engineering. Phishing is one of the most common types of cybercrime (Safi & Singh, 2023; Goenka *et al.*, 2023; Asiri *et al.*, 2023). Preventative measures include aggressive safety precaution deployment, protecting endpoints, frequent software upgrades, and continuous knowledge upgrading for employees. Biometric Authentication (Debas *et al.*, 2023; Khan *et al.*, 2023), Advanced Thread Detection (Ullah *et al.*, 2019), Endpoint security solutions, CAPTCHA (Awasthi *et al.*, 2019), use of blockchain for enhanced security features (Demirkan *et al.*, 2020; Hasanova *et al.*, 2019; Hassani *et al.*, 2018; Truong *et al.*, 2023) are some of the advanced ways banks can predict and prevent cyberattacks.

6. References

AAG IT Support. (n.d.). The latest cyber crime statistics. https://aag-it.com/the-latest-cyber-crime-statistics/

Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, *4*(1), Article tyy006. https://doi.org/10.1093/cybsec/tyy006

Alabdan, R. (2020). Phishing attacks survey: Types, vectors, and technical approaches. *Future Internet*, *12*(10), Article 10. https://doi.org/10.3390/fi12100168

Asiri, S., Xiao, Y., Alzahrani, S., Li, S., & Li, T. (2023). A survey of intelligent detection designs of HTML URL phishing attacks. *IEEE Access*, *11*, 6421–6443. https://doi.org/10.1109/ACCESS.2023.3237798

Awasthi, S., Srivastava, A. P., Srivastava, S., & Narayan, V. (2019). A comparative study of various CAPTCHA methods for securing web pages. *2019 International Conference on Automation, Computational and Technology Management (ICACTM)* (pp. 217-223). https://doi.org/10.1109/ICACTM.2019.8776832

Bamrara, A., Singh, G., & Bhatt, M. (2013). Cyber attacks and defense strategies in India: An empirical assessment of banking sector. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2488413

Berjawi, O., Attar, A. E., Chbib, F., Khatoun, R., & Fahs, W. (2023). Cyberattacks detection through behavior analysis of internet traffic. *Procedia Computer Science*, *224*, 52-59. https://doi.org/10.1016/j.procs.2023.09.010

Blaze. (2023). B*iggest cyber threats for financial institutions in 2023*. https://www.blazeinfosec.com/post/cyber-threats-for-finance-2023/

Brooks, C. (n.d.). *Cybersecurity Trends and Statistics For 2023; What You Need To Know*. Forbes. https://www.forbes.com/sites/chuckbrooks/2023/03/05/cybersecurity-trends--statistics-for-2023-more-treachery-and-risk-ahead-as-attack-surface-and-hacker-capabilities-grow/

Cavelty, M. D., Eriksen, C., & Scharte, B. (2023). Making cyber security more resilient: Adding social considerations to technological fixes. *Journal of Risk Research*, *26*(7), 801-814. https://doi.org/10.1080/13669877.2023.2208146

Cherqi, O., Moukafih, Y., Ghogho, M., & Benbrahim, H. (2023). Enhancing cyber threat identification in open-source intelligence feeds through an improved semi-supervised generative adversarial learning approach with contrastive learning. *IEEE Access*, *11*, 84440-84452. https://doi.org/10.1109/ACCESS.2023.3299604

Crane, C. (2023). A look at 30 key cyber crime statistics. *Hashed Out by The SSL Store*^{TM}. https://www.thesslstore.com/blog/cyber-crime-statistics/

Debas, E. A., Alajlan, R. S., & Hafizur Rahman, M. M. (2023). Biometric in cyber security: A mini review. *2023 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)*, 570-574. https://doi.org/10.1109/ICAIIC57133.2023.10067017

Demirkan, S., Demirkan, I., & McKee, A. (2020). Blockchain technology in the future of business cyber security and accounting. *Journal of Management Analytics*, *7*(2), 189-208. https://doi.org/10.1080/23270012.2020.1731721

Donalds, C., & Osei-Bryson, K.-M. (2020). Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents. *International Journal of Information Management*, *51*, Article 102056. https://doi.org/10.1016/j.ijinfomgt.2019.102056

Dwyer, A. C., Stevens, C., Muller, L. P., Cavelty, M. D., Coles-Kemp, L., & Thornton, P. (2022). What can a critical cybersecurity do? *International Political Sociology*, *16*(3), Article olac013. https://doi.org/10.1093/ips/olac013

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2022). Detecting insider threat via a cyber-security culture framework. *Journal of Computer Information Systems*, *62*(4), 706-716. https://doi.org/10.1080/08874417.2021.1903367

Goenka, R., Chawla, M., & Tiwari, N. (2023). A comprehensive survey of phishing: Mediums, intended targets, attack and defence techniques and a novel taxonomy. *International Journal of Information Security*, *23*, 819-848. https://doi.org/10.1007/s10207-023-00768-x

Hasanova, H., Baek, U., Shin, M., Cho, K., & Kim, M.-S. (2019). A survey on blockchain cybersecurity vulnerabilities and possible countermeasures. *International Journal of Network Management*, *29*(2), Article e2060. https://doi.org/10.1002/nem.2060

Hassani, H., Huang, X., & Silva, E. (2018). Banking with blockchain-ed big data. *Journal of Management Analytics*, *5*(4), 256-275. https://doi.org/10.1080/23270012.2018.1528900

Hindustan Times. (2023). *Financial fraud top cyber crime in India; UPI, e-banking most targeted: Study*. https://www.hindustantimes.com/business/financial-fraud-top-cyber-crime-in-india-upi-e-banking-most-targeted-study-101695036325725.html

Hussen, N., Elghamrawy, S. M., Salem, M., & El-Desouky, A. I. (2023). A fully streaming big data framework for cyber security based on optimized deep learning algorithm. *IEEE Access*, *11*, 65675-65688. https://doi.org/10.1109/ACCESS.2023.3281893

Iscan, C., Kumas, O., Akbulut, F. P., & Akbulut, A. (2023). Wallet-based transaction fraud prevention through LightGBM with the focus on minimizing false alarms. *IEEE Access*, 1-1. https://doi.org/10.1109/ACCESS.2023.3321666

Khan, H. U., Malik, M. Z., Nazir, S., & Khan, F. (2023). Utilizing bio metric system for enhancing cyber security in banking sector: A systematic analysis. *IEEE Access*, *11*, 80181-80198. https://doi.org/10.1109/ACCESS.2023.3298824

Kumar, A., & Om, H. (2018). An improved and secure multiserver authentication scheme based on biometrics and smartcard. *Digital Communications and Networks*, *4*(1), 27–38. https://doi.org/10.1016/j.dcan.2017.09.004

Malinka, K., Hujňák, O., Hanáček, P., & Hellebrandt, Luk. (2022). E-banking security study—10 years later. *IEEE Access*, *10*, 16681-16699. https://doi.org/10.1109/ACCESS.2022.3149475

Mijwil, M., Salem, I. E., & Ismaeel, M. M. (2023). The significance of machine learning and deep learning techniques in cybersecurity: A comprehensive review. *Iraqi Journal For Computer Science and Mathematics*, *4*(1), Article 1. https://doi.org/10.52866/ijcsm.2023.01.01.008

Mohammad, R. M., Thabtah, F., & McCluskey, L. (2015). Tutorial and critical analysis of phishing websites methods. *Computer Science Review*, *17*, 1-24. https://doi.org/10.1016/j.cosrev.2015.04.001

Palatty, N. J. (2022). *90+ Cyber Crime Statistics 2023: Cost, Industries and Trends*. https://www.getastra.com/blog/security-audit/cyber-crime-statistics/

Pan, Y., Ge, X., Fang, C., & Fan, Y. (2020). A Systematic literature review of android malware detection using static analysis.

IEEE Access, *8*, 116363-116379. https://doi.org/10.1109/ACCESS.2020.3002842

Porcedda, M. G. (2023). Sentencing data-driven cybercrime. How data crime with cascading effects is tackled by UK courts. *Computer Law and Security Review*, *48*, Article 105793. https://doi.org/10.1016/j.clsr.2023.105793

Safi, A., & Singh, S. (2023). A systematic literature review on phishing website detection techniques. *Journal of King Saud University - Computer and Information Sciences*, *35*(2), 590-611. https://doi.org/10.1016/j.jksuci.2023.01.004

Security Intelligence. (2023). *Cost of a data breach 2023: Financial industry impacts*. https://securityintelligence.com/articles/cost-of-a-data-breach-2023-financial-industry/

Statista. (n.d.). *Cost of a data breach in financial sector worldwide 2023*. https://www.statista.com/statistics/1324063/cost-of-data-breaches-in-financial-industry-worldwide/

Truong, V. T., Le, L., & Niyato, D. (2023). Blockchain meets metaverse and digital asset management: A comprehensive survey. *IEEE Access*, *11*, 26258-26288. https://doi.org/10.1109/ACCESS.2023.3257029

Ullah, F., Naeem, H., Jabbar, S., Khalid, S., Latif, M. A., Al-turjman, F., & Mostarda, L. (2019). Cyber security threats detection in internet of things using deep learning approach. *IEEE Access*, *7*, 124379-124389. https://doi.org/10.1109/ACCESS.2019.2937347

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, *62*(1), 82-97. https://doi.org/10.1080/08874417.2020.1712269