American Journal of Computer Science and Technology
2022; X(X): XX-XX
http://www.sciencepublishinggroup.com/j/ajcst
doi: 10.11648/j.XXXX.2022XXXX.XX
ISSN: 2640-0111 (Print); ISSN: 2640-012X (Online)

Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking

Diptiben Ghelani[1], Tan Kian Hua[2], Surendra Kumar Reddy Koduru[3]

[1]Institute of Computer Science, Gujrat Technological University, Ahmedabad, India.

[2]Management and International Business, and Cyber Security, LIGS University, Honolulu, USA

[3]Department of Information Technology, Allahabad Agricultural Institute, Allahabad, India

Email address:

shezi1131@gmail.com

To cite this article:

Diptiben Ghelani. Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking. *American Journal of Computer Science and Technology*. Vol. x, No. x, 2022, pp. x-x. doi: 10.11648/j.xxx.xxxxxxxx.xx

Received: MM DD, 2022; **Accepted**: MM DD, 2022; **Published**: MM DD, 2022

Abstract: We live in a time when data security has become a significant concern. Cyber services are the most enjoyable and time-saving aspects of one's life. On the other hand, people save their data in the cloud, handled by the cyber. In this case, cyber-security is quite vital. This is an open security challenge because many intruders can attack the data and hack the user's details through the server. If we look around, we will see a lot of cases involving cyber-crime. The security of our cloud-based datasets has become a serious concern. Our research will include data security, including intruder detection that can happen anywhere on the planet. Protecting data from intruders has become critical, and intruder detection should be the essential key to identifying. How will we know who is stealing the data that has been secured using biometric security, fingerprints, passwords, OTPs, and other methods if we don't know who the intruder is? Intruder detection has become increasingly important, particularly on mobile objects such as aeroplanes and ships. We can only find a solution if we understand the problem. We employ machine learning, biometric recognition, data learning, and hybrid approaches to avoid this. These will be the system's handles, and they will help secure data from intruders by utilizing the best optimization techniques to obtain precise data. We proposed a banking system model in which biometric impressions and digital signatures are used to enable every transaction by a bank's customer. This proposal recommends that the Smart Online Banking System (SOBS) be made more secure by employing biometric prints, which decreases the number of threats that an invader may pose.

Keywords: Cyber Security, Banking, Programming, Framework

1. Introduction

Cyberbanking and cyber security are terms used to describe technologies, practices, and processes that protect data, networks, and computer programmes from cyber-attacks. A cyber security threat is a type of financial terrorism that has become increasingly prevalent. The most challenging aspect of modern cyberbanking has been protecting customers' personal information. Cyber security is a strategy for preventing cyber-attacks in cyberspace. A breach in any cyber security system results in financial and non-financial losses for the victim organization and its customers, so cyber security aims to prevent these losses [1]. Theft of intellectual property and sensitive consumer information such as identification numbers and account numbers are examples of non-financial losses. Cybercrime is a global issue with severe economic consequences for South African society. Securing sensitive information is a critical concern regarding cyber security and privacy in the cyberbanking domain [2]. With technology at the forefront, the banking sector has transformed, with internet banking becoming a more convenient means of doing business. South African banks frequently use third-party platforms such as PayPal to conduct international and domestic transactions. Because the administration of these systems is out of the banks' control, their dependence on third-party systems to supply sure of their digital services to clients poses a severe security risk. As systems become more tightly connected, reliance grows, as does the risk of cyber breaches or assaults. Controlling these threats entails limiting and mitigating attacks before they occur, known as risk management.

Deloitte has opened a Cyber Intelligence Centre (CIC) in Nairobi, Kenya, the first of its kind in Africa, and provides world-class cyber security solutions. The centre is linked to other centres on seven continents utilizing cutting-edge technology. Beginning in June 2016, this centre will assist businesses in developing a risk-based, proactive cyber security plan that will aid in the prevention, detection, and response to cyber-attacks [3].

1.1. Deloitte CIC Offers the Following Services

1.1.1. Cyber Monitor

A real-time security information and event management solution that will detect, analyze, alert, report, and initiate a response process 24 hours a day, seven days a week;

1.1.2. Cyber Watch

A threat intelligence feed that is accurate and personalized to spot potential attacks before they happen; Continuous vulnerability scanning and control is provided by Cyber Check.

1.1.3. Cyber Respond

responds to cyber events and defends the organization's systems and networks. Banks' traditional risk management strategies frequently concentrated on intercepting a single point of attack. However, as the digital world evolves, an assault can now concurrently target several systems and processes, resulting in massive financial consequences for the institution. Cyberbanking is becoming an increasingly important aspect of the Internet of things (IoT), and these platforms come with their own set of security concerns. IoT refers to a network of physical things that can gather and share data. These objects can include gadgets, buildings, and other stuff. As IoT becomes increasingly prevalent in everyday life, privacy and security concerns grow. Cyber-attacks are a hazard that can occur in today's technological environment due to a lack of cyber security knowledge on users' side. The physical world is becoming one extensive information system due to the Internet of Things, with the ultimate objective of increasing quality of life and enabling new economic models [4]. Traditional communication security measures have been used to combat cyber-attacks, with authentication and access control giving some granularity to the first layer of defence. These strategies have been ineffective because they must be combined with other security measures such as procedural and personal security controls. Information systems (IS) have recently been exposed to rapidly changing surroundings in the Internet age [5]. The frequency of assaults, for example, varies with time, such as workdays and vacations; abuses and attacks go with user and hacker expertise. As a result, the risk of information systems is not the same for all places. A countermeasure may be effective at one moment but ineffective at another. Defending IS against danger is incredibly expensive and has a high failure rate. A functioning IS must analyze the profile of IS assaults over time and provide appropriate security countermeasures that are proportional to the present danger, allowing the IS to protect itself effectively and at little expense. In this circumstance, making all security decisions at design time isn't enough; instead, security information must be managed during run time [6]. It is also proven that, rather than depending on ad hoc security techniques, companies require a high level of awareness and systematic management of security issues [7].

Security risk management is a knowledge-intensive process that necessitates the Monitoring and capture of important data that may aid managers in making the best choice possible. A semantically improved paradigm for security management over the lifecycle of an information system is provided in this study [8]. The model enables the continuous collection of identified threat behaviours from an intrusion detection system, the filtering and analyzing threats within a time snapshot, and the re-appraisal of IS security countermeasures with the security administrator (S-Admin), managers, and the IS and security management system as stakeholders. The probe agent uses the created ontology-driven knowledge base to categorize the security risks discovered by the IDS [9]. In contrast, long-term frequency probability was used to determine the possibility of threats happening in real time. The offered security solutions are based on CASE, a threat ontology that already exists. The re-appraiser is based on the possibility of continued threats succeeding [10]. The system assists management in making security control selection decisions so that they may maximize their Return on Security Investment. An e-banking system demonstrates the suggested Collect–Probe–Analyze–Reason–Reappraise approach [11].

In today's world, as experience has demonstrated, securing state information security in the banking sector plays a critical role in safeguarding Ukraine's national security, particularly its economic component (BNC). Theory and practice play a key and system-forming role in the process of developing a system for providing bank information (BIn) as a component of the state's national information resources, in which the scientific and methodological foundation serves as the foundation for making informed and effective management decisions by entities providing state budget at all levels [12]. The last decade's revolutionary changes in the banking sector have resulted in the unification of information and computer networks into single information and cybernetic space, resulting in the creation of automated banking systems that have significantly expanded the range of electronic services offered by state and commercial banks around the world, including in Ukraine. As a result, risks to the state's national information resource, BIn, have drastically changed. Threats have begun to blend. Because of the simultaneous influence on the target of protection, hybridization of threats such as information security (IS), cyber security (CS), and security of information (SI) began to emerge [13].

1.2. Analysis of the Nature and Content of Information Security Problems

The transition from an information society to a high-tech community in the early twenty-first century is characterized

by the oversaturation of new information and communication technologies, further development of globalization in the modern economy, and the dynamics of information in such areas of society as communication, energy, transportation, system production and storage of oil and gas, financial and banking systems [14]. Second, information processes worldwide emphasize the importance of information security. This is especially important given the status of its information resources, the rising market value of information, its high susceptibility, and the frequent considerable losses resulting from unlawful usage. Third, the fast growth of the Internet and other information and communication technologies is transforming the global information environment, resulting in new dangers and forms of international conflicts, such as information warfare, network confrontation, and hacking [15]. The advancement of computer technology and information and telecommunication networks offers tremendous potential to society, creating a new type of crime known as cybercrime.

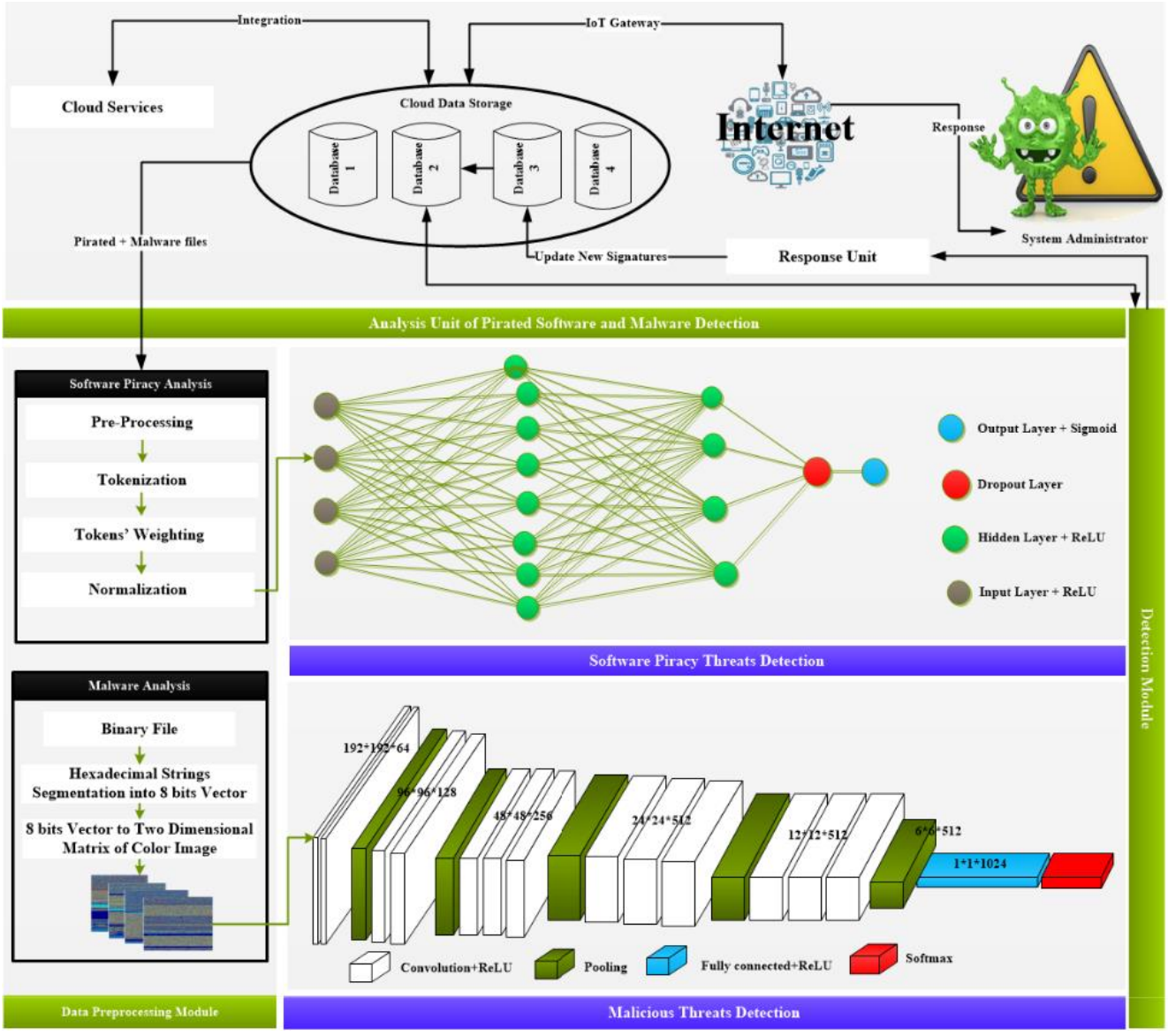

Figure 1. *IoT cyber security threat prediction architecture model.*

2. Literature Review

The standard deviations of the Discrete Wavelet Transform (DWT) coefficients of the entire picture at different levels and familiarization make up the feature vector proposed by Tico et al. For matching, a K-Nearest Neighbor classifier with Euclidean distance is utilized. Many intruder attackers are waiting to take advantage of the bank's customers. More clients will feel comfortable using online banking if the banking system is more secure. Junho Lee, Jungwoon Woo, and his colleagues presented a technology by offering an application and a technique for producing software to establish a safe online. It lacks the OOAD approach, UMLsec, and Java EE to manage the database and link it with correlations. Wazid, Zeadally, and Das highlighted the

necessity for mobile banking and every conceivable attack when utilizing the mobile banking system in the malware threats and security solutions session [16]. They have demonstrated their work in mobile banking, its limits and advancements, but no model for securing it has been developed. Similarly, R. Bose, S. Chakraborty, and S. Roy described the working concept of multi-factor cloud authentication architecture for a financial system that uses biometric fingerprint authentication through USB to ensure data authenticity. Even though they set up a secure and safe VPN connection, they could not protect the data from various cyber-attacks [17].

2.1. An Examination of the Nature and Scope of Information Security Issues

The terrorist organization "Islamic State of Iraq and Greater Syria" (ISIS) developed a cyber assault team in 2015. Attacks on Internet resources, including banks, research institutions, public organizations, and others, are common in this Internet sector known as the Cyber Caliphate, whose major aims are evil and the revelation of secret information. The cost of acceptable and effective remedies can be assessed by the degree of threat electronic crimes provide to society. According to specialists in electronic document security in the United States, the overall cost of protecting a bank or other financial institution might be as little as 510 thousand dollars. However, a big financial institution's security system, which serves up to 80,000 customers and is valued at least $ 15 million (excluding hardware and software costs), is rated trustworthy (excluding the salaries of state employees' own security company) [17]. Threats to information can take many different forms. The goal of serious instability of public order characterizes cyber terrorism. This phenomenon is directly tied to the development of information infrastructure, as society's continued progress is dependent on the flawless operation of computer systems. Actions targeted at their destruction inflict more severe harm and elicit a strong public response [17]. This refers to targeted cyber terrorism aimed at intimidating the public and authorities and actual or potential effects on cybernetic society, socio-technical, and technical systems, the commission of which causes (creates conditions for) danger to citizens, society, and state. The use of terrorism to carry out terrorist operations using current information resources, especially the Internet, has been a cause of great worry in the previous decade [18]. The properties of the Global Network attract terrorist groups. In this scenario, FRA or BFA will be utilized to collect data to authenticate the smart online banking system. It facilitates the acquisition of a picture for preprocessing through fingerprints/face recognition/digital signature. The following stage will be feature extraction, using whatever picture the system has acquired as input through preprocessing and image acquiring gateway. The received image will be analyzed by an SVM classifier or a training classifier, which will assist in generating a judgement, either to validate or reject the user. Rejected input will be used to feed the machine again, while acceptable input will allow users to manage their account transactions [19]. The suggested model will function, allowing an authorized user to transact in the financial system. Anything can be done intelligently, and no validation can rule out BFA or FRA. These are the most well-known technologies for enhancing transaction security. This also makes the current banking system safer than the current internet banking system. Within the suggestion of the candidate region, the act of CNN as a feature extractor and the dense layer, which is comprised of output from the image extractor, serves to provide input to the SVM that classifies the object's existence. Additionally, this suggested approach will boost the bounding box's prediction to assist create offset value to extract the precise data of the user to forecast the object's presence. In comparison to its predecessors, CNN has the advantage of robotically detecting critical traits without the need for human experience or supervision [20]. It consists of Preprocessing and Image Obtaining, Feature Extraction with the aid of Neural Networking or features of Region-Based with Convolution Neural Networks (R-CNNs), which helps recognize objects that may be used for deep models, Features Extraction, and Verification. The R-CNN's model selects several existing areas from the picture, such as anchor boxes, bounding boxes, and their labelling categories, such as offsets. They employ CNN for forwarding computation after choosing from the picture to assist extract features from the provided area. Later, each suggested region's characteristic predicts the labelling category and the bounding box. IS security engineering has lately been included in the development process, allowing developers to produce more secure software systems. The final software product will not be secure if focused attempts to protect the programme at the development stage are not made. Meanwhile, real security issues surrounding software system deployment in operational mode are frequently overlooked or moved to intrusion detection and response systems. Security stockholders can model and incorporate such aspects using ontology-based security standards [21]. A security ontology is an improved approach for storing information and acquiring essential knowledge to improve security brands in organizations. Several ontologies-based systems have been presented, and they have helped design novel information system security methods. From an ontological perspective, the focus was on improving IoT cyber security by offering suitable security services tailored to the risks [22].

IS security engineering has lately been included in the development process, allowing developers to produce more secure software systems. The final software product will not be safe if focused attempts to protect the programme at the development stage are not made. Meanwhile, actual security issues surrounding software system deployment in operational mode are frequently overlooked or moved to intrusion detection and response systems. Security stockholders can model and incorporate such aspects using ontology-based security standards [23]. A security ontology is an improved approach for storing information and acquiring essential knowledge to improve

security brands in organizations. Several ontologies-based systems have been presented, and they have helped design novel information system security methods. From an ontological perspective, the focus was on improving IoT cyber security by offering suitable security services tailored to the risks [23].

2.2. The Security Management System and Its Application

The CPARR architecture for security management is detailed in this section. For e-banking security management, the CPARR model is used as a case study. The suggested method is implemented as an IDS-independent plug-in tool with benefits based on simulated attack scenarios. CPARR architecture implementation and validation yielded some promising outcomes. The ontology is built with Protégé OWL, the agent is implemented with JAVA JADE, and the database is built with Oracle SQL Developer [23].

2.3. Introducing the CPARR Architecture in Place for Security Management

A series of real-time data are simulated for the e-banking IDS to evaluate the proper application of CPARR architecture to the e-banking system. Using the simulated IDS results, the suggested plan is checked and validated. Because of the difficulties of obtaining access to the bank's IDS report, the output of the IDS is mimicked. The result is random for 15 different attack scenarios and ten users in various places around an organization. The instrdetect programme was designed to randomly mimic assaults on the login accounts of ten distinct users in ten different areas. The initial-designed security ontology must be populated with organization-specific information through the protégé OWL editor before the system can function correctly[24].

Today's world has made cyber civilization a popular and unavoidable source of information exchange and other professional activities such as business, shopping, bank transactions, ads, services, etc. This exponential rise in internet use has led to an exponential increase in cybercriminal activity. These Web apps include design flaws, which cyber thieves exploit to obtain unauthorized access to systems. As a result, cyber security has become a significant issue for both scholars and practitioners [25]. Cyber security is the collection of tools, techniques, policies, security measures, security guidelines, risk mitigation strategies, activities, training, good practices, security reassurance, and cutting-edge technology that may be utilized to secure cyberspace and users' assets. Cyber security is becoming an issue of worldwide interest and importance, and it entails safeguarding data by detecting, avoiding, and responding to cyber-attacks. Various firms' defensive methods for protecting their cyberspace are insufficient to defend their cyber environments from ever-increasing security risks [26]. As a result, it is one of the significant scientific concerns that has drawn the attention of scholars and practitioners during the previous decade. Various research efforts have been made in numerous cyber areas, each with its own set of traits and quirks for dealing with multiple security breaches. Multiple methodologies and technologies for detecting and mitigating cyber security risks have been proposed in the literature. However, before further additional study in this field, it is necessary to collect the previous work [27].

3. Proposed Framework

There are four aspects to the proposed cyber banking security framework: Controls for operational circumstances, controls for first threat entrance locations, and controls for known dissemination strategies. Figure shows the rules that optimize and validate the threats. This framework's propagation tactics and approaches and its entrance point are related to the network security defensive mechanism. The entrance point identifies the network's access point by separating the outside physical space from the cyberbanking physical area. At the network's entrance, firewalls and routers are installed. The policy manager and the network firewall define and configure the propagation strategies and procedures. The framework's optimization, validation, and operating conditions are related to application security. The notion of least privilege might be used to attain operational requirements. Implementing vulnerability checks in the application might help with optimization and validation. Controls that address operating circumstances include software and hardware purchases, secure software and hardware setup on workstations, laptops, and servers, and continual vulnerability evaluation and repair. Cyber security defence strategies, application-level security, mobile and wireless device management, data recovery capability plans, and security skill evaluation and training are among the controls that address first attack entry points [28]. Rules for known propagation strategies configure network devices, including firewalls, switches, and routers. Access control to network ports, services, protocols, administrative privilege management, border defence implementation, security audit log maintenance, Monitoring and analysis Monitoring and management of accounts, security incident response capabilities, and data recovery capabilities are among the controls that optimize and validate risks [29].

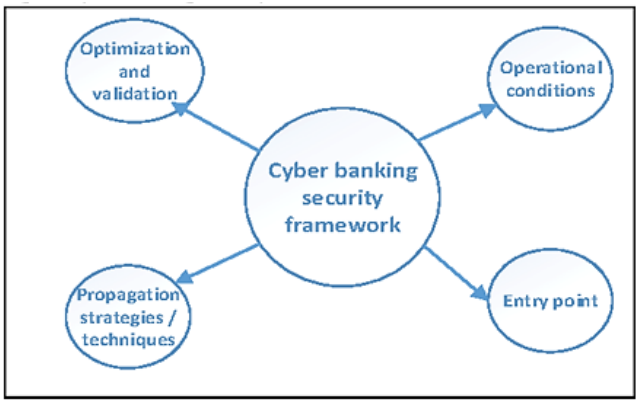

Figure 2. *Cyber Banking Security Framework.*

3.1. Cyber Security Terminologies

The following are some definitions of essential terminologies required to understand better the main ideas associated with the study topic. Cyberspace is a worldwide realm within the information world characterized by the electronic and electromagnetic spectrum to generate, update, store, distribute, and exploit information via linked and dependent networks utilizing cutting-edge information and communication technology [30].

3.1.1. Vulnerabilities

These are weaknesses in a system or its design that allow an attacker to execute malicious instructions, get unauthorized access to data, and carry out different denial-of-service attacks [28].

3.1.2. Threats

These are measures performed to profit from security flaws in a system while negatively impacting it [31].

3.1.3. Attacks

These are the measures performed to cause harm to a system or disrupt its normal functioning by exploiting vulnerabilities with various tools and techniques. Attackers carry out these attacks to fulfil their nefarious objectives, whether for self-satisfaction or financial gain. Several security flaws have been mentioned in the literature [32]. To help readers comprehend some of the most frequent cyber security weaknesses, the following are described:

3.1.4. Denial-of-Service (DoS)

This sort of attack prevents intended users from accessing a machine or network resource. Any event that reduces or destroys a network's ability to execute its anticipated purpose causes it. Most computer devices in the IoT context are vulnerable to asset enervation attacks due to their low memory capacity and limited processing resources. One of the causes of a DoS attack is that different businesses employ similar technology, which prospective attackers exploit [33].

3.1.5. Malware

The attacker uses malicious software programmers in this attack to obtain unauthorized access to computer systems by exploiting security flaws. The motive behind the malware is a significant financial or political payoff that increases an attacker's drive to infiltrate as many network devices as possible to achieve their harmful goals [34].

3.1.6. Phishing

This is a criminal crime involving social engineering and technology to get sensitive information from an Internet user. Phishing strategies use a variety of communication channels, including email, instant chats, pop-up messages, and Web sites [35].

3.1.7. SQL injection attack

An input string is injected into the application in this attack to update or manipulate the SQL query to the attacker's benefit. This assault causes damage to the database in numerous ways, including illegal database access and modification, as well as the revealing of sensitive data. This attack is dangerous since it might result in data loss or usage by unauthorized organizations, destroying functionality and confidentiality. Furthermore, system-level instructions are executed as part of this type of attack, preventing authorized users from accessing the necessary information. Man-in-the-Middle attacks and session hijacking Man-in-the-middle (MITM), sometimes known as MIM, MitM, MiM, or MITMA in the literature, is an attack in which an unauthorized third party stealthily acquires control of a communication channel between several endpoints. The MITM attacker can disrupt, modify, or even replace the communication flow of the target victims [35].

3.2. Site-to-Site Scripting (XSS)

In this form of attack, a hostile attacker attempts to run JavaScript code in the client's browser to steal sensitive data from the client. It is a frequent vulnerability discovered in current Web pages. Vicious assaults are becoming more common as the number of IoT networks grows. Malware assaults are often designed for compromising the privacy of IoT nodes, computer systems, and cellphones over the Internet. Furthermore, victims are unaware of the invader, believing that the communication connection is secure. Several scanning strategies based on specific signatures are offered to detect Windows-based malware. The malware identification analysis is separated into two approaches: static and dynamic [36].

Malware patterns are discovered using the Dynamic Approach while executing code in a real-time virtual environment. Malicious Conduct Function calls, function parameter research, data flow, instruction traces, and visual code analysis can all be used to detect this. There are automated online tools that may be used to study the dynamic behaviour of dangerous code. Specifically, CW Sandbox, Anubis, and TT analyzer. This approach takes more time since it monitors every dynamic behaviour of the source code. Static malware analysis approaches do not need source code execution in real-time [37]. It might be used to obtain information about the layout of malware binaries. The static malware identification approaches are control flow graph, opcode frequency, n-gram, and string signature. Before using static-based methods, the disassembly tools IDA Pro and OllyDbg are used to reveal the executable. These disassemblers extract hidden patterns from binary executables. These patterns are then utilized to get the encoded text from the executable. The byte sequence methodology is a static-based analytic method for extracting n-byte sequences from these patterns. A functional call graph is a static tool for removing code structural analysis [1].

3.3. Software

3.3.1. Piracy

Because software's intellectual digital property and authorship rights are worldwide available on the Internet,

they are challenging to preserve. Currently, every third software programme installed is pirated. The attacker may breach the original software and rewrite the logic in a different programming language. Because each programming language has different syntax and semantic frameworks, detecting crackers' harmful actions in cross-domain source codes is challenging. Tools available can convert one form of source code to another, such as MoHCA-Java. Because open-source programmes were readily available, it was simple for crackers to steal the original idea and develop their software. One cannot be compensated for his views but rather for his capacity to give answers in the actual world [38].

3.3.2. Malware Detection

Traditional approaches may address code obfuscation problems. However, texture feature mining utilizing virus visualizations has a high computational cost. These feature extraction approaches do not work well with large amounts of malware data. Malware is constantly being created, updated, and manipulated, making detection more difficult. The majority of cutting-edge work is done in a single programming language. For example, if a cracker changes the control flow of source code to another data structure in a comparable programming language, the current literature is helpful. The software benchmark was utilized to detect danger in java source code. It retrieved structural characteristics by extracting the control flow of source programmes. To determine the similarity, the benchmarks of two source codes were compared [39].

As a result, it can give important insights into malware. The author developed a beneficial clustering-based technique in which many malware samples may be automatically scaled into groups/classes of clusters based on their execution behaviour. They expanded the Anubis system to perform more network analysis and tainted tracking to provide automatic monitoring reports for the chosen malware strains. Their enhanced approach was able to characterize various programme actions more abstractly. Hybrid techniques are presented to address time and computational cost concerns and improve malware detection systems. They dubbed their technique OPM because they employed static and dynamic information taken from malware samples to train a malware classifier. They regarded static characteristics as operational code frequency occurrences [40].

On the other hand, dynamic features might include execution traces of executable files and system calls. The findings show that the hybrid strategy performs significantly better as a combined approach than independently running static and dynamic methods. Much research has been conducted to enhance the performance of classification findings and reduce time, size, and resource overhead. For example, presented a malware classification algorithm based on CNN and images. This method had a classification accuracy of 98.52 per cent. It randomly selected 10% of the malware family's samples for testing. A deep learning model for malware detection was created by Reference. For 9339 malware samples, the suggested method obtained 98 per cent classification accuracy. The CNN approach is introduced in this paper for malware classification. The proposed method achieved 94.5 per cent classification accuracy [41-48].

4. Conclusion

Thus, the models and methods proposed in this work allow for the construction of effective mechanisms for the protection of cyber security in banking systems at the canonical, logical, and physical levels of their representation, limiting access and admission to the content of their data to only those with appropriate user authority, and establishing rules for user interaction with information resources based on optimal, requirements-consistent criteria. This provides the most significant possible architecture for easy access and the safest means to protect their data from various threats. Future research will secure this model against unforeseen dangers and make it more user-friendly. As cyberbanking is becoming more evolved and becoming more and more digital, management of big data becomes more critical. The storage of this big data will rely on technologies such as the cloud. Risks and threats should be contextualized, and a realistic evaluation of what may go wrong should be part of security management. To do so, a thorough understanding of what has gone wrong with the systems over time and the types of persistent assaults and their implications is essential.

References

[1] Panja, B., et al. Cybersecurity in banking and financial sector: Security analysis of a mobile banking application. in 2013 international conference on collaboration technologies and systems (CTS). 2013. IEEE.

[2] Jibril, A. B., et al. Customers' perception of cybersecurity threats toward e-banking adoption and retention: A conceptual study. in ICCWS 2020 15th International Conference on Cyber Warfare and Security. 2020. Academic Conferences and publishing limited.

[3] Johnson, A. L., Cybersecurity for financial institutions: The integral role of information sharing in cyber attack mitigation. NC Banking Inst., 2016. 20: p. 277.

[4] Uddin, M., M. Ali, and M. K. Hassan, Cybersecurity hazards and financial system vulnerability: a synthesis of literature. Risk Management, 2020. 22 (4): p. 239-309.

[5] Rodrigues, A. R. D., et al., ARTIFICIAL INTELLIGENCE, DIGITAL TRANSFORMATION AND CYBERSECURITY IN THE BANKING SECTOR: A MULTI-STAKEHOLDER COGNITION-DRIVEN FRAMEWORK. Research in International Business and Finance, 2022: p. 101616.

[6] Kerr, G., Cybersecurity in Banking and Payments in the United Kingdom. The VISIO JOURNAL, 2018: p. 39.

[7] Mohammed, D., Cybersecurity compliance in the financial sector. The Journal of Internet Banking and Commerce, 1970. 20 (1): p. 1-11.

[8] Bryant, L., Cybersecurity regulations: Banking and third party providers. 2016, Utica College.

[9] Berdyugin, A. A. and P. V. Revenkov, Approaches to measuring the risk of cyberattacks in remote banking services of Russia. Безопасность информационных технологий, 2019. 26 (4): p. 83-92.

[10] Thach, N. N., et al., Technology Quality Management of the industry 4. 0 and Cybersecurity Risk Management on Current Banking Activities in Emerging Markets-the Case in Vietnam. International Journal for Quality Research, 2021. 15 (3): p. 845.

[11] He, W., X. Tian, and J. Shen. Examining Security Risks of Mobile Banking Applications through Blog Mining. in MAICS. 2015.

[12] Zabala Aguayo, F. and B. Ślusarczyk, Risks of banking services' digitalization: The practice of diversification and sustainable development goals. Sustainability, 2020. 12 (10): p. 4040.

[13] Al Duhaidahawi, H. M. K., et al., The financial technology (fintech) and cybersecurity: Evidence from Iraqi banks. International Journal of Research in Business and Social Science (2147-4478), 2020. 9 (6): p. 123-133.

[14] Lyeonov, S., et al., The innovative approach to increasing cybersecurity of transactions through counteraction to money laundering. Marketing, 2019 (3): p. 309.

[15] Augustinos, T. P., Developing cybersecurity requirements in banking (And Other financial services). Banking LJ, 2018. 135: p. 155.

[16] Dam, L., Relationship Between Demographic Variables and Awareness on Cybersecurity Threats: An Empirical Analysis. The Orissa Journal of Commerce, 2020. 41: p. 112-122.

[17] ur Rehman, T., Cybersecurity for E-Banking and E-Commerce in Pakistan: Emerging Digital Challenges and Opportunities, in Handbook of Research on Advancing Cybersecurity for Digital Transformation. 2021, IGI Global. p. 163-180.

[18] ur Rehman, T., A Study of Advancing E-Banking and Cybersecurity for Digital Enterprise Transformation in Pakistan, in Handbook of Research on Advancing Cybersecurity for Digital Transformation. 2021, IGI Global. p. 267-287.

[19] Naseer, A., et al., Real-time analytics, incident response process agility and enterprise cybersecurity performance: A contingent resource-based analysis. International Journal of Information Management, 2021. 59: p. 102334.

[20] Toapanta, S. M. T., J. M. E. Jaramillo, and L. E. M. Gallegos. Cybersecurity analysis to determine the impact on the social area in Latin America and the caribbean. in Proceedings of the 2019 2nd International Conference on Education Technology Management. 2019.

[21] Nawa, E. -L. T., Developing a cybersecurity framework for the banking sector of Namibia. 2021, Namibia University of Science and Technology.

[22] Kuzmenko, O. V., Trends of fraud operations on the banking market and approaches of cybersecurity assessment. 2020.

[23] Williams, R. T., Banking and Cybersecurity Governance. 2021, Utica College.

[24] Olmstead, K. and A. Smith, Americans and cybersecurity. Pew Research Center, 2017. 26 (311–27).

[25] Al Duhaidahawi, H. M. K., et al., Analysing the effects of FinTech variables on cybersecurity: Evidence form Iraqi Banks. International Journal of Research in Business and Social Science, 2020. 9 (6): p. 123-133.

[26] Ashiku, L. and C. Dagli. Cybersecurity as a centralized directed system of systems using SoS explorer as a tool. in 2019 14th Annual Conference System of Systems Engineering (SoSE). 2019. IEEE.

[27] Voas, J., et al., Cybersecurity Considerations for Open Banking Technology and Emerging Standards. 2022, National Institute of Standards and Technology.

[28] Swain, S. C., Cybersecurity Threats and Technology Adoption in the Indian Banking Sector: A Study of Retail Banking Customers of Bhubaneswar. Strategies for e-Service, e-Governance, and Cybersecurity: Challenges and Solutions for Efficiency and Sustainability, 2021: p. 51.

[29] Ng, A. W. and B. K. Kwok, Emergence of Fintech and cybersecurity in a global financial centre: Strategic approach by a regulator. Journal of Financial Regulation and Compliance, 2017.

[30] Kshetri, N. and J. Voas, Banking on availability. Computer, 2017. 50 (1): p. 76-80.

[31] Rehman, T. U., Digital Transformation of E-Commerce Services and Cybersecurity for Modernizing the Banking Sector of Pakistan: A Study of Customer Preferences and Perceived Risks, in Handbook of Research on Advancing Cybersecurity for Digital Transformation. 2021, IGI Global. p. 373-403.

[32] Nunes, E., et al. Darknet and deepnet mining for proactive cybersecurity threat intelligence. in 2016 IEEE Conference on Intelligence and Security Informatics (ISI). 2016. IEEE.

[33] Chlela, M., et al., Fallback control for isochronous energy storage systems in autonomous microgrids under denial-of-service cyber-attacks. IEEE transactions on smart grid, 2017. 9 (5): p. 4702-4711.

[34] Stevens, C., Assembling cybersecurity: The politics and materiality of technical malware reports and the case of Stuxnet. Contemporary Security Policy, 2020. 41 (1): p. 129-152.

[35] Lim, S. K., et al. Malwaretextdb: A database for annotated malware articles. in Proceedings of the 55th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers). 2017.

[36] Hasham, S., S. Joshi, and D. Mikkelsen, Financial crime and fraud in the age of cybersecurity. McKinsey & Company, 2019: p. 1-11.

[37] Camillo, M., Cybersecurity: Risks and management of risks for global banks and financial institutions. Journal of Risk Management in Financial Institutions, 2017. 10 (2): p. 196-200.

[38] Kancherla, K. and S. Mukkamala. Image visualization based malware detection. in 2013 IEEE Symposium on Computational Intelligence in Cyber Security (CICS). 2013. IEEE.

[39] Ghelani, D., & Hua, T. K. (2022). Conceptual Framework of Web 3.0 and Impact on Marketing, Artificial Intelligence, and Blockchain. *International Journal of Information and*

Communication Sciences, *7*(1), 10.

[40] Ghelani, D., & Hua, T. K. A Perspective Review on Online Food Shop Management System and Impacts on Business.

[41] Ghelani, D., Hua, T. K., & Koduru, S. K. R. (2022). A Model-Driven Approach for Online Banking Application Using AngularJS Framework. *American Journal of Information Science and Technology*, *6*(3), 52-63.

[42] Dr. John Ughulu. The role of Artificial intelligence (AI) in Starting, automating and scaling businesses for Entrepreneurs.. *ScienceOpen Preprints.* DOI: 10.14293/S2199-1006.1.SOR-.PP5ZKWJ.v1

[43] Ughulu, J. Entrepreneurship as a Major Driver of Wealth Creation.

[44] Oak, R., Du, M., Yan, D., Takawale, H., & Amit, I. (2019, November). Malware detection on highly imbalanced data through sequence modeling. In *Proceedings of the 12th ACM Workshop on artificial intelligence and security* (pp. 37-48).

[45] Hua, T. K., & Biruk, V. (2021). Cybersecurity as a Fishing Game: Developing Cybersecurity in the Form of Fishing Game and What Top Management Should Understand. Partridge Publishing Singapore.

[46] Vasan, D., et al., Image-Based malware classification using ensemble of CNN architectures (IMCEC). Computers & Security, 2020. 92: p. 101748.

[47] Gupta, A., S. Gupta, and R. Katarya, InstaCovNet-19: A deep learning classification model for the detection of COVID-19 patients using Chest X-ray. Applied Soft Computing, 2021. 99: p. 106859.

[48] Ghelani, D., & Gillani, D. H. (2022). A perspective study on Malware detection and protection, A review. *Authorea Preprints*.

[49] Lad, S. S. and A. C. Adamuthe, Malware Classification with Improved Convolutional Neural Network Model. International Journal of Computer Network and Information Security (IJCNIS), 2020. 12 (6): p. 30-43.