Spectrum Journal of Innovation, Reforms and Development
Volume 40, June 2025 | ISSN (E): 2751-1731
WEBSITE: WWW.SJIRD.JOURNALSPARK.ORG

A FINANCIAL AND BANKING PERSPECTIVE ON THE SIGNIFICANCE OF CYBERSECURITY IN FISCAL AND MONETARY POLICIES IN THE DIGITAL AGE

1Mohammed Madlool Ali Al-Sultan
bus.mohammed.madl.ool@uobabylon.edu.iq

2Nooraldeen Sabah Mahdi Kmalaldeen
Nooraldeen.sabah@uobabylon.edu.iq

3 Hayder Mohammed Kareem Al Shebly
bsc.haider.muhammed@uobabylon.edu.iq

1, 2, 3Department of Economics, Faculty of Administration & Economics, University of Babylon, Babylon, Iraq

Abstract

The research focused on the concept of cyber security, its importance in financial and monetary institutions, the most prominent tools followed by cyber security, the challenges and digital attacks that these institutions are exposed to by hackers and financial fraud criminals via the Internet. It also focused on the most important applications and solutions followed by cyber security in these institutions as economic, financial and monetary policies to prevent digital fraud. The digital challenges and attacks that financial and banking institutions are exposed to, whether through financial fraud, malware, threats, hacking, etc., require adopting appropriate solutions and enhancing cyber security tools and applications, which refer to the security of the network, programs, applications, information, and infrastructure, in addition to flexibility, governance, and cyber security awareness, as well as raising awareness among employees and customers of financial and banking institutions, adopting multi-factor authentication, biometric data, automatic logout, strong firewalls, etc.

Keywords: Cyber security, cyber security challenges, financial and banking institutions, financial and monetary cyber security applications.

Introduction

Two decades ago, the term cyber security was unknown to the general public. In the current digital era, the rise of cyber security was significant not only for people, users, and consumers, but also for businesses, regulations, financial and monetary institutions, and the banking and economic sectors in all of its manifestations. Everything has recently been digitalised with the use of several contemporary computer applications and technology. But contemporary technology may also lead to cyberattacks and risks to security, privacy, and financial and monetary funding. Based on this, the study clarifies the idea of cyber security, its significance in the changing policy and financial and monetary institutions environment, and its vital role in using efficient instruments to combat

digital threats to these institutions and policies. Countering electronic assaults, securing data against theft, interception, and encryption, and preventing computer access, theft, and content hacking are the main objectives of cybersecurity research. Therefore, via certain applications, it may be able to shield banks and organisations from any outside cyber security intrusion.

Literature Review:

The subject of cybersecurity and its connection to financial institutions has been covered in a variety of literary works. The rise in financial fraud, the increase in the value of digital financial and monetary assets, the expansion of banking and financial services, and the capacity to handle cybersecurity challenges have all contributed to the growing interest of academics in researching this significant topic from a variety of angles, especially from a financial and monetary perspective. Here are a few literary works that have tackled this subject:

According to Nagasundari Selvara's article, the substantial rise in financial fraud and cybercrime has made the implementation of strong security measures necessary to guarantee online safety. As financial technology advances, internet users' attention to cyber security has grown significantly in relation to everyday transactions and activities including investing, exchanging money, making purchases, and more.

This paper concluded that there is a need for cooperation by institutions and governments and international participation, which would enhance the efficiency and effectiveness of cyber security. Future research can also highlight its importance in exploring the obstacles organizations face during the cyber security implementation process, and the key performance indicators that organizations can rely on to ensure the ultimate goal is achieved [1].

According to the study presented by Neelam Sethi, server hacking and theft of customer personal information, along with cyber fraud (PII), has become commonplace. This study aims to highlight the importance of cyber security in the banking industry, given that most people and companies conduct their business online, the risk of a data breach is almost constantly increasing. Therefore, the study focused on the role of cyber security in banking operations and specialized banking software such as Secure Socket Layers (SSL) for TCP/IP connections.

Two-factor authentication and changing passwords to strong passwords that include difficult-to-hack symbols, letters, and numbers have helped limit cyber activities [2]. Amy Kay (2017) critically analyzed cyber threats in the financial and banking sector and encouraged financial sectors to adopt measures and technologies to prevent and control these attacks. Any institution, whether financial, banking, or otherwise, must adopt strict electronic security policies and measures to limit these malicious attacks, and constantly update protection tools and device security management [3].

Between Chandra Sekhara and Manoj Kumar Kumar, the banking sector witnesses an escalation of cyber-attacks and cybercrimes such as fraud, hacking, and forgery from multiple sources, computers being one of them. It was reported that 50% of cybercrimes are related to ATMs, debit cards, and online banking services. These crimes can be prevented by ensuring authentication, verification, and identification technologies. Cyber security is a key weapon in combating cybercrime in digital banking, by providing security measures to protect users' accounts of digital money, such as debit and credit cards, transactions, and financial operations [4].

First: The Concept of Cyber security:

The term cyber security is commonly used by computer and information technology specialists, digital economy leaders, digital financial and banking institutions, digital technology businesses, industry professionals, and national security practitioners [5].

A collection of situations or occurrences pertaining to enhancing the integrity of a digital information management system or infrastructure and tackling digital issues via the internet are often referred to as cyber security. It appears nearly hard to come to a consensus on a single definition because it covers such a wide range. Cyber security is also the process of implementing best practices and technologies to defend critical infrastructure, cyberspace, and critical systems of people, institutions, and organizations against potential digital attacks that legally violate property rights [6]. In order to ensure confidentiality, integrity, and availability, it is also a collection of technologies, policies, security concepts, security safeguards, guidelines, risk management techniques, procedures, training, best practices, and tools that can be used to defend networks, computers, software, data, and the cyber environment against damage, attack, and unauthorized access [7].

Cyber security is a comprehensive, specialized, and dynamic field that is used to protect systems, communication networks, and digital data, preventing unauthorized access to systems and data and cyber attacks, to secure these digital data and electronic systems from fraud and cyber attacks to ensure their safety [8].

There are many principles and fundamentals upon which cyber security is based, such as computer science, information technology, coding, data management, electronic laws and regulations, hacking risk assessment, attack preparedness, and cyber security training for security personnel. Accordingly, the art of cyber security principles consists of three main axes, as follows: [10]

Protecting important and confidential digital data from being disclosed or accessed by unauthorized third parties means protecting that data by using effective and strong encryption and secure and legitimate systems, with this procedure, we ensure that the data remains confidential and secure without being transferred or stored from one person to another and it is also protected from tampering and leakage. This achieves what is known as availability, meaning that data is easily accessible when requested and stored in systems that provide unscheduled interruptions.

Second: Cyber security Importance

Cybersecurity currently plays a significant and effective role in ensuring the safety, stability, and strengthening trust of all institutions and systems that interact with technology. With the increasing need for digital security, data protection has become an absolute necessity, not an optional one. Therefore, the importance of cyber security arises as follows:

- **Complete protection of sensitive and confidential information: Data stored online is vulnerable to multiple cyber-attacks, so cyber security ensures its protection.**
- **Preserving Privacy**: Whether it's individuals or large institutions, privacy relies on securing digital information. Strong cybersecurity keeps personal data safe from identity theft and other breaches.
- Data privacy: It is the reliance on complete security of digital data and its protection from theft and attacks.

- Arming Infrastructure: Many vital institutions, such as healthcare, banking, and transportation, rely entirely on digital data. Cybersecurity protects them safely.
- **Financial Protection: Ransomware and cyberattacks cause significant economic and financial damage. Cybersecurity works to protect against this.**
- **National Security: Cybersecurity protects sensitive systems from attacks, such as payment, internal, and intelligence systems.**
- **Ensuring Business Continuity**: Financial and commercial organizations depend on reliable digital operations. Security measures protect them from outages or breaches that could halt activity.
- **Combating Cybercrime**: As digital crimes grow, cybersecurity provides the first line of defense—helping prevent attacks and track down those responsible.

In short, cybersecurity underpins the stability and resilience of our digital lives. Without it, both daily convenience and national security are at risk.

Maintaining Trust: In the digital world, trust is essential. Therefore, by showcasing a dedication to safeguarding personal data and guaranteeing a safe online environment, cyber security measures are crucial in fostering and preserving confidence among users, clients, partners, and financial and banking institutions. Therefore, it can be argued that, in the digital age, cyber security is not just a technical requirement but also a crucial component of preserving domestic and international security, economic, financial, and monetary stability, and the overall well-being of people, organizations, and financial and banking institutions in the face of the constantly changing digital threat landscape. It also ensures that their assets are protected from potential incidents or other security breaches.

Third: Cyber security Tools

Protecting devices, programs, and data against hackers and digital attacks that try to steal money, change or delete important data, etc., is why cyber security is a must rather than a choice. There are a number of fundamental cyber security technologies that may be described as follows in order to offer the best possible protection for such data, equipment, and applications [12]:

Firewalls: One of the most crucial instruments for cyber protection is a firewall. Their main purpose is to keep unauthorized people out of private networks that are linked to the internet. They may come in the form of software, hardware, or a mix of both. By reviewing all incoming communications and blocking those that don't adhere to security rules, a firewall filters all messages coming into and going out of the internal network.

Antivirus software: to remove viruses and malware from personal computers, most notably Trojan horses.

- **Antivirus Software**: Automatically updates to detect new threats in real time. It also scans emails to block harmful attachments.
- **PKI Services (Public Key Infrastructure)**: Uses encryption and digital certificates to ensure secure data exchange and verify identities online.
- **Network Security Monitoring and Management**: Tools like firewalls, intrusion detection systems, and packet analyzers help monitor networks and spot vulnerabilities.

- **Managed Detection and Response (MDR)**: Offers advanced threat detection, incident analysis, and response. It's especially useful for organizations with limited resources.
- **Penetration Testing**: Cybersecurity experts simulate attacks using hacker-like methods to find weaknesses. These tests help identify where a system can be exploited and provide guidance for fixing those flaws.
- **Web Vulnerability Scanners**: Automatically check websites for security gaps like SQL injections or cross-site scripting. The results include detailed risk reports and solutions.

Employee Education or Training: Employee training is not a direct tool for cyber security, but it can be an effective tool in defending against illegal attacks and threats. When employees possess sufficient cyber security knowledge and awareness, this reduces the risk of online security breaches for public and private organizations and companies operating in all sectors. Thus, it can be noted that without a strong cyber security team, no company, financial institution, or banking institution can avoid the risks and challenges of the internet. Hackers are constantly searching for security vulnerabilities to exploit. Therefore, when it comes to protecting sensitive and private data held by companies, financial institutions, and individuals, cyber security plays a crucial and effective role in mitigating these harmful digital threats and attacks [13].

Fourth: Cyber security Challenges in Financial and Banking Institutions

Given the evolution of financial and monetary institutions from traditional procedures to the modern digital technology era, and the use of computers, mobile devices, and other digital tools, this has opened up various channels and threats to financial and banking institutions, whether to their integrity, financial systems, sensitive data, or the decline in user and customer confidence. The primary cyber security challenges facing financial and banking institutions include the following:

Financial Fraud: Financial fraud poses a widespread threat to financial and banking institutions, their clients, and users. This includes various forms, such as account takeover, such as unauthorized access to customer accounts, fraudulent payment transactions, counterfeit checks, or fraudulent bank transfers. This fraudulent activity can lead to significant financial losses and legal consequences for affected parties.

Insider Threats: Insider threats, whether intentional or accidental, pose significant risks to the online security of financial and banking institutions, as they involve malicious or negligent actions by users within the financial or banking institution. These threats can manifest in various forms that are difficult to detect and prevent, as they target trusted individuals within the financial or banking institution [15].

Unencrypted Data: This type of threat is common in digital financial and banking services, where data is left unencrypted and unhidden. Hackers or cyber attackers can easily exploit this data, creating serious problems for digital financial and banking services [16].

Malware: This popular hacking method entails infecting consumers' devices with harmful malware via the internet. Financial, banking, and electronic payment systems are seriously threatened by compromised computers and mobile devices. Using such software has the drawback of making it simple for hackers to get access to the system and steal substantial amounts of money from payment gateways and banks without being detected or leaving any evidence of their intrusion [17].
Third-party services: To improve service, a lot of banks and other financial institutions employ third-party services. The information of those financial and banking organizations can be readily compromised if a user gives their banking information, including their ATM PIN, CVV, and OTP codes, to a third party [18].

Identity theft and spoofing: This is the latest form of cyber threat facing digital financial and banking services. Internet hackers mimic the URL of a banking website to appear as if it were the original site. When a user accesses their login window, the hackers steal the details of those financial and banking institutions and use them later.

Tampered Data: Hackers can more easily deceive people into sending money through electronic payment systems under false pretences when they change data pertaining to cyber security systems. This results in financial losses for banks and financial organizations. Phishing: The oldest and most prevalent cyber threat, this technique uses email, phone calls, SMS messages, and other means to try and gain private information including ATM PINs, card verification codes, one-time passwords, credit or debit card data, and more.

Ransom ware: Online banking services are being threatened by ransom ware. Via hacked websites, malicious downloads, or email attachments, malware can infect a user's device. After installation, it can lock users out of their accounts and demand a payment to unlock them; record keystrokes, or steal login information. Attacks using ransom ware have the potential to seriously impair banking and financial services and result in large losses [19].
Hackers utilize social engineering as a technique to trick and expose private information in order to get money or gain access to private data. To make it more likely that someone will click on links, download malware, or believe a bad source, social engineering can be used in conjunction with any of the aforementioned risks [20].

Account Takeover: An account takeover happens when hackers or cybercriminals access a user's bank account without authorization. They have the ability to move money, make purchases, or engage in financial fraud, making the account holder susceptible to identity theft and financial loss.
Attacks by a Man-in-the-Middle (MitM): Cybercriminals utilise man-in-the-middle attacks to intercept user communications with the web platform of a bank or other financial institution. Malware on the user's device or hacked Wi-Fi networks can do this. Criminals can alter the content of messages, redirect transactions, or get login credentials during these assaults without the user's awareness [21].

Trojan Horses: Before being downloaded onto a computer, hackers may employ a variety of dangerous tactics known as Trojan horse attacks to fool users into granting them access to secure data. Although a banking Trojan looks like a trustworthy software, it is actually a virus that is intended to gain access to private data that is processed or saved by online banking systems [21]. Figure (1) provides insight into the types and percentage of attacks and digital crimes against financial and banking institutions in the US economy in 2023. It shows that, of all attacks, credit card fraud accounted for the largest percentage at 39%, while other attacks accounted for the lowest percentage at 1%.

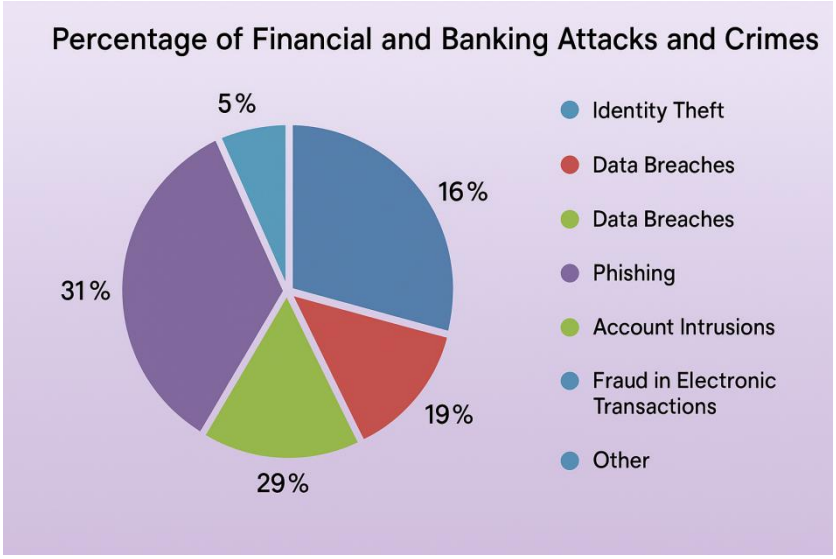

Figure (1) Percentage and Type of Attacks on Financial and Banking Institutions in the United States

We note from Figure (2) that the financial losses resulting from cybercrimes and attacks on financial and banking institutions in the US economy amounted to $12.5 trillion in 2023. This is a significant loss and a historic peak compared to $17.8 trillion in 2001. It is noted that there is a continuous increase in digital attacks and financial and monetary damage to these institutions, as confirmed by the Internet Crime Complaint Center (IC3) in the United States.

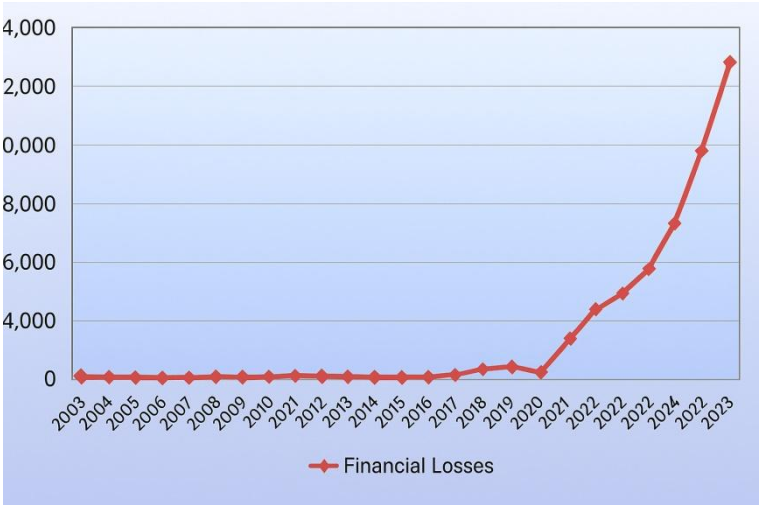

Figure (2) Losses and Damages to Financial Institutions in the United States

Digital attacks cause damage to financial and banking institutions worldwide. Figure (3) shows that the percentage of damage caused by these digital attacks on financial and banking institutions reached 34% of the total attacks and data breaches in 2021, while it increased significantly in 2024, recording a 65% increase, double the 2021 figure. This represents a serious threat to the stability of these financial and banking institutions.

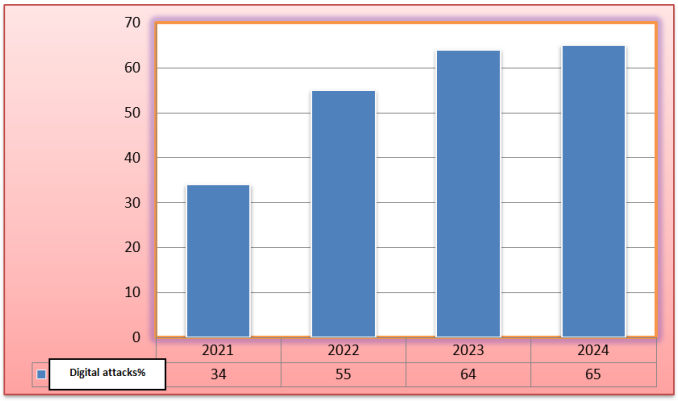

Figure (3) Digital Attacks on Financial and Banking Institutions Worldwide

Fifth: Cyber security Applications in Financial and Banking Institutions

The technological innovations and digital development of the twenty-first century, on the one hand, and the growth of online financial services, mobile transactions, and digital banking services, on the other, are the main reasons why cyber security is so important in financial and banking institutions. A thorough cyber security plan is necessary for this. As a result, cyber security has become a key component in safeguarding the availability, confidentiality, and integrity of financial and banking data in international financial and banking sectors and institutions. It also helps to protect these sectors and institutions from ransom ware attacks, financial fraud, data breaches, and other malicious attacks.

Finance and banking cyber security

Digital transformation has changed the way we control and engage with financial services; it has also offered fresh avenues for cyber dangers. In banking and finance, cyber security is not only technological; it is also necessary for confidence, stability, and continuity. Here is a brief summary:

• **Its Significance:** Cyber risks go beyond monetary loss. They undermine public confidence and have the power to upset whole institutions. So, cyber security is a basis rather than only defense.

• **Basic Defiance Zones:**

Scans for unusual activities to prevent breaches early.

o Software Security: Protects vital services and applications from defects and harmful code.

o Risk Management: Finds and lessens system weaknesses.

o Cyber Resilience: Guarantees institutions can bounce back fast from assaults.

Awareness Training: Teaches clients and employees to lower human mistake.

Cyber Governance: Matches security with corporate strategy and rules.

o Information Security: Safeguards private consumer and employee data.

o Infrastructure Security: Creates multilayer defences to stop unauthorised access.
o Application and Cloud Security: Especially in digital settings, it protects services and platforms.

- **IoT Security:** Guards linked gadgets that might reveal access points.
- **Important Answers:** One-time codes, biometrics, and passwords combine to form Advanced Authentication (MFA).
- **End-to-End Encryption:** Ensures unreadable, secure communication for outsiders.
- **Behavioural Analytics:** Identifies anomalous user activity that could indicate fraud.

The Larger View:

Digital fraud is on the rise 65% of assaults in 2024 were aimed at banks putting the financial industry under great stress. Cybercrime cost the U.S. $12.5 trillion in 2023. Leading cause of losses was credit card fraud, which accounted for 39 percent.

Now a crucial component in banking, cyber security is without it, both banks and their clients are exposed. It helps us to guarantee continuity and confidence in addition to systems.

Conclusion:

Cyber security is now a strategic pillar in banking. Without it, both institutions and their customers stand vulnerable. With it, we secure not only systems, but also confidence and continuity.

References:

1. Nagasundari Selvara , THE ESSENCE OF CYBER SECURITY THROUGH FINTECH 3.5 IN PREVENTING AND DETECTING FINANCIAL FRAUD: A LITERATURE REVIE Electronic Journal of Business and Management e-ISSN:2550-1380-ISSN , Vol.6 Issue 2, 2021.
2. Neelam Sethi ,CYBER SECURITY ANALYSIS IN BANKING SECTOR international Journal of Advanced Research in Commerce, Management & Social Science (IJARCMSS) 59 ISSN : 2581-7930, Impact Factor : 5.880 , Volume 04, No. 03(I), July - September, 2021,.
3. Amy Kay, How financial institutions address cyber security threats: A critical Analysis , issue in Information Systems Volume 22, Issue 1, 2021.
4. Chandra Sekhar, Manojkumar Kumar , An Overview of Cyber Security in Digital Banking Sector, East Asian Journal of Multidisciplinary Research (EAJMR), Vol. 2, No. 1, 2023.
5. Morten Bay, What is Cyber security In search of an encompassing definition for the post-Snowden era, French Journal For Media Research, ISSN 2264-4733, 2016 .
6. [6] - Francesco Schiliro , Towards a Contemporary Definition of cyber security, Australian Defense Force Academy, University of New South Wales, Canberra 2Macquarie University 21 November 2022 .
7. Dan Craigen ,eat, Defining Cyber security, Technology Innovation Management Review, 1 October 2014 .
8. Shalom joseph, Williams fred, Cyber security in the Digital Age: Protecting Information and Systems,2023 . https://osf.io/preprints/osf/9bxcz
9. Abu Rayhan, Cyber security in the Digital Age: Assessing Threats and Strengthening Defense, Technology Innovation Management Review , 30 April 2024 .

10. Sathyabama Institute of science and technology (deemed to be university) Accredited a grade by NAAC 12 Status by UGC Approved by acute SCHOOL OF Computing Department of Information Techno log , 2020 .
11. Basholli and Juraev , Framework Tools and Challenges in Cyber security, Karshi Multidisciplinary International Scientific Journal Vol. 1(1) 2024 .
12. Kalyani and Rengarajan, cyber security in the Financial Sector , International Journal of Research Publication and Reviews, Vol 5, no 3, March 2024 .
13. Fernando Zopounidis , Cyber security in Online Banking: Challenges and Solution, Journal of Internet Banking and Commerce, Vol. 29, No. 2, March 2024 .
14. JACOB OBAFEMI FATOKI , The influence of cyber security on financial fraud in the Nigerian banking industry, International Journal of Science and Research Archive, 09(02), 2023.
15. Williams Haruna, eat , Defending against cyber security threats to the payments and banking system, 2022 . https://arxiv.org/abs/2212.12307
16. Ashkan Kazem, Origins of Cyber Security: Short Report, international Journal of Reliability, Risk and Safety: Vol. 6, Issue 2, 2023 .
17. L.Mythili and KIRUTHIKA, An Overview of Cyber security in Banking Secto, international Journal of Creative Research Thoughts (IJCRT) www.ijcrt.org , Volume 11, Issue 12 December 2023.
18. Philip Olaseni Shoetan and Babajide Tolulope Familoni, CYBER SECURITY IN THE FINANCIAL SECTOR: A COMPARATIVE ANALYSIS OF THE USA AND Nigeria, Computer Science & IT Research Journal, Volume 5, Issue 4, April 2024.
19. Balaji Dhashanamoorthi, Artificial Intelligence in combating cyber threats in Banking and Financial services,International Journal of Science and Research Archive, 04(01), 2021 .
20. Janusz Pochmara and Aleksandra ´Swietlicka , Cyber security of Industrial Systems—A 2023 Report, Electronics 2024 .
21. https://www.mdpi.com/journal/electronics
22. Manasi Sutar and Mayuri Talegaonkar, Review of Cyber Security Threat in Banking Sector during Covid-19 Pandemic, nternational Journal of Advanced Research in Science, Communication and Technology (IJARSC) Volume 2, Issue 2, June 2022.