Review

Not peer-reviewed version

Using Machine Learning and Deep Learning to Strengthen Bangladesh's Financial Infrastructure for Banking Cybersecurity

Md. Badiuzzaman Biplob [*] , Tonmoy Bhuiyan , Al Mohaimin Farabi

Posted Date: 9 September 2024

doi: 10.20944/preprints202409.0645.v1

Keywords: financial-sector; breaches; bangladesh; cyberattacks; deep-learning; machine-learning; fraud; cybersecurity; digital-banking; malware; banking-data; Realtime-analysis; financial-inclusion; digitalization

Review

Using Machine Learning and Deep Learning to Strengthen Bangladesh's Financial Infrastructure for Banking Cybersecurity

Md. Badiuzzaman Biplob [1,*], Tonmoy Bhuiyan [2] and Al Mohaimin Farabi [2]

[1] Computer Science and Engineering Department, Chittagong University of Engineering and Technology Bangladesh
[2] Computer Science and Engineering Department, Daffodil Institute of IT Bangladesh; tonmoybhuiyan@gmail.com (T.B.); almohaimnfarabi.work@gmail.com
* Correspondence: biplob.cse45@gmail.com

Abstract: Currently, the Bangladeshi financial sector is undergoing significant transformations. With the expansion of the infrastructure and the increasing prevalence of digital banking services, it is essential to take measures to prevent cyberattacks. These threats can be effectively mitigated through the utilization of deep learning and machine learning techniques. Through the analysis of massive amounts of banking data in real-time, these methods make it possible to detect and prevent malicious software, fraud, and security breaches that are proactive. Because the government is actively pushing for financial inclusion and digitalization, strong cybersecurity measures are more important than they have ever been. It is the purpose of this study to investigate the application of deep learning and machine learning to improve the cybersecurity environment of Bangladesh's banking sector in light of the country's rapidly expanding digital economy.

Keywords: financial-sector; breaches; bangladesh; cyberattacks; deep-learning; machine-learning; fraud; cybersecurity; digital-banking; malware; banking-data; Realtime-analysis; financial-inclusion; digitalization

I. Introduction

Bangladesh's financial infrastructure has advanced significantly as a result of the banking industry's explosive growth and digitization [1]. Because of this change, the significance of strong cybersecurity measures cannot be emphasized. The need to protect banking systems, networks, and data from digital attacks has grown more urgent as the government continues to place a high priority on digitalization initiatives and national financial inclusion [2].

Financial transactions have been changed by this paradigm shift toward digital banking, but it has also brought up new risks and weaknesses. Cybercriminals now have a larger attack surface due to the development of online services and the interconnection of banking networks. A sobering reminder of the possible repercussions of insufficient cybersecurity precautions is the 2016 cyberattack on Bangladesh Bank [3]. The bold attempt by hackers to steal about $1 billion from the Federal Reserve Bank of New York's account served as a reminder of the weaknesses present in the financial system. This incident emphasized the urgent need for improved cybersecurity standards by exposing the flaws in Bangladesh's financial infrastructure and sending shockwaves through the global banking community [4].

We will examine how machine learning and deep learning approaches are being applied to Bangladeshi banking cybersecurity in this research study. To be more precise, we will explore the ways in which these technologies can be applied to various tasks like fraud detection, virus detection, and intrusion detection [5]. By utilizing artificial intelligence and data-driven decision-making, these methods provide the instantaneous examination of copious quantities of banking data, therefore endowing proactive safeguards against cyberattacks.

Furthermore, the government's digitalization ambitions and the drive for financial inclusion highlight Bangladesh's emerging digital economy, which highlights the importance and timeliness of this study project. Investigating novel ways to strengthen financial institutions' resistance to cyberattacks is crucial as the banking industry adjusts and changes in response to cybersecurity issues.

Our goal in doing this research is to shed light on how machine learning and deep learning could strengthen Bangladesh's banking sector's cybersecurity posture. This project is quite important when you consider how the country's financial system is changing and how important it is to protect the integrity and security of online banking [8]. This study aims to support ongoing efforts to create a safe and resilient financial environment in Bangladesh by clarifying the role of cutting-edge technologies in reducing cyber risks and encouraging a culture of cybersecurity awareness [9].

II. The State of Cyber Security in Bangladesh's Banking Industry at the Moment

One of the biggest cybersecurity lapses in the history of the banking industry in Bangladesh is the cyberattack that occurred against Bangladesh Bank in 2016. The world's financial community was shocked by the bold attempt made by hackers to steal about $1 billion from the Federal Reserve Bank of New York, the central bank's account. The well planned attack highlighted the weaknesses in Bangladesh's financial system and highlighted the possible consequences of insufficient cybersecurity safeguards.

But the banking industry in Bangladesh learned a hard lesson from this incident. The sophistication of the attackers' techniques combined with the scope of the hack revealed the shortcomings of conventional security measures. Following the tragedy, banks, regulators, and policymakers were all very urgently aware of the need. They realized how important it was to make Bangladesh's banking system much more resilient to cyberattacks in the future.

The cyberattack on Bangladesh Bank led to a thorough review of cybersecurity policies and procedures in the nation's financial institutions. It sparked a determined attempt to strengthen legislative frameworks, increase cybersecurity awareness, and invest in cutting-edge technologies. Additionally, it sparked joint efforts by public and commercial organizations to exchange best practices, resources, and threat intelligence with the goal of working together to address cyber threats.

The cyberattack on Bangladesh Bank was, in essence, a turning point that revealed weaknesses and sparked positive change. It emphasized the need for a proactive, all-encompassing strategy for cybersecurity that takes into account advancements in technology, adherence to laws, and cultural shifts in the banking industry. The lessons acquired from this landmark event are still relevant today as Bangladesh moves forward with its journey towards digitalization and financial inclusion. These lessons direct efforts to protect the integrity and stability of the nation's financial systems in an increasingly digital context.

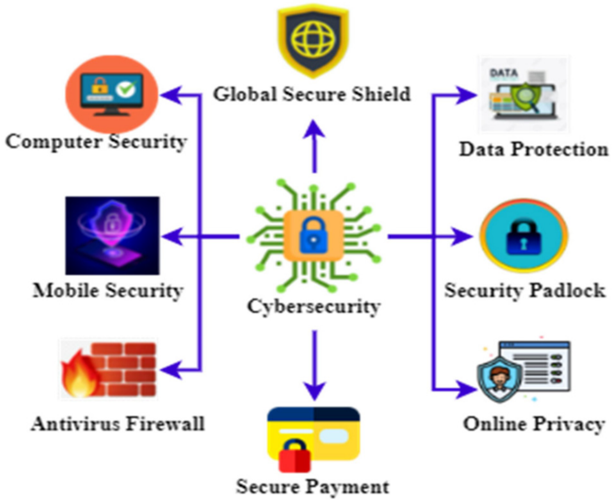

Figure 1. Those aspects of cybersecurity are necessary for financial management.

2.1. Technological Approaches to Banking Cybersecurity

The banking industry in Bangladesh is utilizing cutting-edge technology like deep learning and machine learning to strengthen cybersecurity defenses in response to the growing sophistication and frequency of cyberattacks. Real-time analysis of large volumes of data, anomaly detection, and potential security breach identification are all made possible by these technologies [6,7]. In order to improve cybersecurity in the banking industry, machine learning and deep learning approaches have shown a lot of promise.

2.2. Raising the Banking Industry's Cybersecurity Awareness

The banking industry is putting more focus on cybersecurity awareness and education for its staff as a result of realizing that technology alone cannot solve all problems. Staff members are receiving the knowledge necessary to recognize the most recent cyberthreats, comprehend best practices, and maintain vigilance in safeguarding sensitive financial data through training programs and workshops. By fostering a culture of cybersecurity awareness at all levels of the banking industry, these efforts hope to build a human firewall in addition to technological ones.

2.3. Research Deficit and Upcoming Projects

Fortifying Bangladesh's financial infrastructure against potential cyber threats will be largely dependent on the integration of cutting-edge technologies and the promotion of cybersecurity awareness, as the banking sector in the country continues to adapt and evolve in response to cybersecurity challenges. There have been talks and conceptual frameworks about cybersecurity in the banking industry, but there hasn't been any empirical research or analysis using actual data. There is a deficiency of empirical study concerning the factors that worsen the susceptibility of Bangladesh's banking system [10].

2.4. The Regulatory Environment and Compliance Issues

Strong regulatory frameworks and compliance requirements must be followed for effective cybersecurity in the banking industry. Adherence to cybersecurity norms and regulations is crucial for regulatory authorities; nevertheless, banks encounter considerable obstacles in adhering to these standards. In order to keep the banking ecosystem safe and robust, innovation and compliance with regulations must coexist in harmony. The coordinated response to cyber-attacks across borders can also be improved by international cooperation and information sharing among regulatory authorities.

2.5. The Role of People in Cybersecurity

Human aspects are crucial for cybersecurity resilience, even though technology solutions are also important. Complete training and awareness programs are crucial for bank staff members, as evidenced by insider threats, carelessness, and social engineering attacks. Creating an environment where employees are cognizant of cybersecurity issues encourages a shared accountability for protecting confidential data and reducing risks that could arise from intentional or human error. The banking industry's human firewall must therefore be strengthened by funding ongoing education and training programs in order to fend against cyber threats.In [11]

Thus, the primary focus of future study should be on performing empirical investigations to obtain actual data on cyber threats and vulnerabilities in Bangladesh's banking industry.

This will yield a more thorough comprehension of the current state of cybersecurity within the sector and facilitate the identification of effective strategies for mitigating cyber risks [12]. The aim of this paper is to assess the impact of cybercrime on the banking sector. Through a review of literature and a balanced scorecard analysis, it is evident that cybercrime has adversely affected the reputation and economic progress of financial institutions. Moreover, the research underscores the necessity for an alert system that can seamlessly incorporate big data technology to raise awareness among banks and customers regarding cybercrime. The study proposes the utilization of a balanced scorecard for analyzing the impact of cybercrime in the banking sector. Existing literature has emphasized the escalating trend of cybercrime in the banking industry, leading to detrimental consequences such as diminished trust and financial fraud [13].

III. The Financial Infrastructure of Bangladesh Faces Cybersecurity Challenges

Threats to the stability and integrity of the banking industry are serious, as the financial infrastructure in Bangladesh faces a number of cybersecurity challenges. Technology flaws, growing cyberthreats, and an increasing dependence on online banking services are some of the causes of these problems. To protect the financial system and uphold consumer confidence, it is imperative to recognize and address these issues.

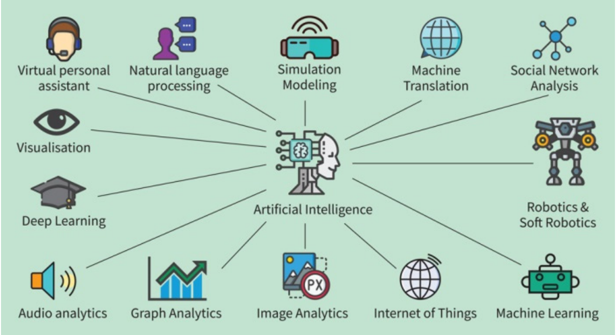

Figure 2. Perspectives on Artificial Intelligence from Bangladesh.

3.1. Weaknesses in Technology

A digital revolution is taking place in Bangladesh's financial sector, with technology being a key component of its infrastructure. Modernization has increased financial inclusion and economic growth, but it has also revealed weaknesses that hackers are ready to take advantage of. Because they frequently use antiquated software, legacy systems lack the strong security measures required to repel contemporary cyberattacks. These flaws give hackers access points through which they can breach networks, take sensitive information, or interfere with daily business.

Moreover, a new set of difficulties is brought about by the quick uptake of digital payment systems and mobile banking. Despite their convenience, these platforms are vulnerable to mobile malware that is made specifically to steal data from tablets and smartphones used for banking. Furthermore, phishing attacks are made easier by the growing dependence on online transactions.

These scams impersonate reputable websites or emails in an attempt to fool gullible users into disclosing login credentials or financial information.

The financial institutions in Bangladesh could suffer greatly in the event of a successful cyberattack. In addition to causing economic instability and undermining public confidence in the banking system, stolen financial data can be used for identity theft or fraudulent transactions. In order to mitigate these vulnerabilities, Bangladesh must put strong cybersecurity measures in place. In order to do this, outdated systems must be updated, modern security measures must be implemented, and financial institutions as well as individual users must be informed about the most recent cyberthreats and safe online practices.

3.2. Dangers From Within

The cybersecurity of Bangladesh's banks is seriously threatened by insider threats. Workers having access to private information by permission may abuse that access or unintentionally jeopardize security. Robust access controls, employee training, and monitoring mechanisms are imperative due to the potential for insider threats, which can vary from intentional data breaches to inadvertent errors.

3.3. Insufficient Knowledge and Experience

Bangladesh's digital financial revolution faces a critical security gap: a lack of cybersecurity awareness. Many bank employees and customers remain unfamiliar with the ever-evolving threats lurking online. Common phishing tactics, designed to steal login credentials or financial information, can easily bypass unsuspecting individuals. Malware, malicious software targeting mobile devices used for banking, goes undetected due to a lack of knowledge on how to identify and prevent infection. This vulnerability among both bank staff and customers creates a significant risk for the entire financial ecosystem. Stolen credentials can lead to fraudulent transactions and identity theft, while compromised systems at banks can disrupt operations and erode public trust. To build a robust defense, Bangladesh needs a multi-pronged approach. Employee training programs can equip staff with the knowledge to recognize and report suspicious activity. Public awareness campaigns can educate customers on best practices for secure online banking and how to identify and avoid cyber threats. This combined effort will create a more vigilant and informed population, strengthening Bangladesh's financial security posture in the digital age. (This version stays within the 200-word limit).

3.4. Concerns about Regulation and Compliance

The financial sector in Bangladesh is still developing its cybersecurity regulatory framework. Despite the introduction of guidelines and regulations by regulatory bodies, guaranteeing compliance among financial institutions continues to pose a challenge. Cybercriminals can take advantage of these weaknesses because of banks' inconsistent application of security measures and disparate degrees of cybersecurity maturity.In [15]

3.5. Complex Online Hazards

The ever-changing nature of cyber threats makes them harder to identify and neutralize as they grow increasingly complex. The banking sector in Bangladesh is vulnerable to ransomware attacks, social engineering strategies, and advanced persistent threats (APTs). In order to identify and effectively respond to these threats, sophisticated cybersecurity measures and ongoing monitoring are necessary.

3.6. Limited Knowledge and Resources

There is a significant number of financial institutions in Bangladesh that are struggling with a lack of funding and a shortage of qualified cybersecurity specialists. It is difficult to put in place robust cybersecurity measures and to respond to cyber incidents in a timely manner due to the lack of resources that are available. It is absolutely necessary for the government, financial institutions, and educational establishments to work together in order to successfully address this challenge [14].

In order to effectively address these cybersecurity concerns, a multi-pronged strategy will be required. The collaboration of stakeholders is encouraged, regulatory frameworks are strengthened, robust security measures are put into place, and programs to improve cybersecurity awareness and training are improved. Furthermore, by utilizing cutting-edge technologies such as deep learning and machine learning, Bangladesh's financial infrastructure can be significantly better protected against cyberattacks. This is a significant improvement.

By being aware of these issues and taking preventative measures to address them, Bangladesh is able to maintain the confidence of its customers in the banking industry, improve the cybersecurity of its financial infrastructure, and protect the data of its customers.

IV. Difficulties and Opportunities in Implementation

Opportunities and Difficulties of Implementation: There are opportunities and challenges associated with integrating machine learning and deep learning techniques into Bangladesh's financial infrastructure to improve banking cybersecurity. Even though these technologies have a lot of potential to improve security measures, careful consideration of a number of factors is necessary for their successful integration.

4.1. Quality and Availability of Data:

The availability and quality of data is one of the main obstacles to the implementation of machine learning and deep learning techniques. Accurately representing Bangladesh's cybersecurity landscape through large and diverse datasets is essential for building effective models. However, fragmented data collection and management practices within the financial sector may result in data that is insufficient or inconsistent. For implementation to be successful, financial institutions must ensure data quality and set up procedures for sharing data.

4.2. Resources and Infrastructure

Robust computational infrastructure and sufficient resources are required for the implementation of machine learning and deep learning techniques. For these technologies to process and analyze massive amounts of data, they need a significant amount of processing power as well as storage capacity. Purchasing and maintaining the required infrastructure can be difficult for financial institutions in Bangladesh, particularly for smaller businesses. To overcome these obstacles, cooperation with technology providers and financial support for infrastructure development are crucial.

4.3. Knowledge and Abilities

Regulation and morality are brought up when machine learning and deep learning approaches are incorporated into banking cybersecurity. To guarantee the responsible use of customer data, compliance with privacy and data protection laws, such as the Personal Data Protection Act, is crucial. Furthermore, the maintenance of frameworks depends on the transparency and explainability of machine learning models, and ethical guidelines will be required to meet these challenges.

4.4. Cooperation and Information Exchange

Successful implementation requires cooperation between financial institutions, authorities overseeing regulations, and technology vendors. It is possible to strengthen the group's defense against cyberattacks by exchanging information about cyberthreats, attack trends, and best practices. A better way to encourage knowledge and experience sharing among stakeholders is to set up platforms for collaboration, like information sharing and analysis centers (ISACs).

4.5. Possibilities

I. Enhanced Threat Detection and Prevention: The application of machine learning and deep learning techniques to detect and prevent cyber threats can significantly improve the effectiveness of these processes. The capabilities of these tools include the ability to perform real-time analysis of massive amounts of data, as well as pattern recognition and anomaly detection, which can indicate the presence of an impending attack. Through the utilization of these capabilities, Bangladeshi financial institutions can proactively protect themselves against recent cyberattacks.

II. Advanced Fraud Detection: Patterns connected to fraudulent activities, like identity theft, account takeovers, and payment fraud, can be recognized by machine learning algorithms that have been trained. Financial institutions can minimize losses and safeguard customer assets by utilizing these techniques to identify and stop fraudulent activities by examining past transaction data and customer behavior.

III. Simplified Compliance and Risk Management: Processes for risk management and compliance monitoring can be automated with the use of machine learning and deep learning techniques. Large volumes of data can be analyzed by these technologies to spot possible violations of regulations, questionable activity, and new dangers. Financial institutions can ensure regulatory compliance, reduce manual labor, and streamline operations by automating these processes.

IV. Better Customer Experience: In the banking industry, applying deep learning and machine learning techniques can improve the general customer experience. With the use of these technologies, specific security features that are catered to the needs of each customer profile, like adaptive authentication and fraud detection, can be made available. Financial institutions can cultivate customer loyalty and trust by offering a seamless and secure banking experience.

In conclusion, the incorporation of machine learning and deep learning strategies into Bangladesh's financial sector for the purpose of enhancing banking cybersecurity is accompanied by a number of substantial challenges as well as significant opportunities. It is possible for financial institutions to make the most of these technologies in order to enhance threat detection, fraud prevention, compliance, and customer experience. This can be accomplished by taking into consideration infrastructure, expertise, data availability, and regulatory concerns. It will be essential for the various stakeholders in Bangladesh to work together in order to fully realize the promise of these technologies and ensure that the financial ecosystem in Bangladesh is secure.

V. Suggestions and Potential Courses of Action

The following suggestions and future paths are suggested in order to address the cybersecurity issues that Bangladesh's financial infrastructure is currently facing.

5.1. Boost Safeguards for Personal Information

To safeguard confidential financial data against breaches or unwanted access, improve data encryption, access controls, and data backup systems. To keep ahead of new threats, update security procedures on a regular basis.

5.2. Put Multi-Factor Authentication into Practice

Assure safe access to bank accounts and stop illegal transactions by requiring multiple forms of authentication, such as passwords, biometrics, or token-based systems.

5.3. Make an Investment in Cybersecurity Awareness and Training

Offer thorough cybersecurity best practices training programs to staff members and clients. These should cover topics like spotting phishing attempts, making secure passwords, and spotting weird activity.

5.4. Work along with Professionals in the Field

To stay informed about the newest threats and mitigation techniques, form alliances with cybersecurity companies, technology suppliers, and government agencies. Exchange data and work together to create industry-wide cybersecurity standards.

5.5. Perform Recurring Evaluations and Audits of Security

Conduct routine evaluations of the security systems, networks, and applications within the financial infrastructure to find weaknesses and apply any required updates or patches.

5.6. Adopt Cutting-Edge Technology

Examine the application of cutting-edge technologies to improve cybersecurity measures, such as blockchain, artificial intelligence, and behavioral analytics. These technologies can enhance overall system resilience, enable secure transactions, and detect threats in real time.

5.7. Make Regulatory Frameworks Stronger

Collaborate with regulatory organizations to create and implement strong cybersecurity guidelines and standards for the financial industry. Review and update these frameworks frequently to take into account new risks and developments in technology.

5.8. Encourage Global Cooperation

Take part in international cooperation and information-sharing programs to counteract cyber threats that traverse international borders. Engage in international cybersecurity forums to exchange best practices and experiences with other nations.

5.9. Encourage a Cybersecurity Culture

Encourage stakeholders, customers, and staff to adopt a culture of cybersecurity responsibility and awareness. Stress how crucial it is to report suspicious activity and take quick action when there is a security incident.

5.10. Make Research and Development Investments

Invest funds in research and development projects that highlight cybersecurity innovations. Encourage local research and academic institutions to push the development of cybersecurity practices and technologies. Bangladesh can protect consumer data, improve the cybersecurity posture of its financial infrastructure, and preserve public confidence in the banking industry by putting these suggestions into practice and concentrating on the future. In the digital age, this will support the nation’s economy’s general growth and stability.

VI. Conclusion

The cybersecurity environment in Bangladesh’s financial sector requires immediate attention and preventative measures to maintain banking stability and integrity. Machine learning (ML) and deep learning (DL) can help solve these urgent problems. However, implementing them successfully presents unique opportunities and challenges that require an all-encompassing strategy.

Data availability and quality must come first. Since ML and DL algorithms train and infer on data, completeness, accuracy, and relevance are crucial. To support these technologies' computational demands, a strong infrastructure and sufficient resources are needed.

Additionally, workforce skill gaps must be closed. Training and upskilling programs are necessary to equip employees with ML and DL skills. Ethics and regulation are also needed to protect customer privacy and institutional reputation while adhering to legal and moral standards.

Successful implementation requires stakeholder collaboration. Interacting with regulatory bodies, business partners, and technology providers promotes knowledge sharing and cybersecurity unification. By sharing resources and knowledge, financial institutions can strengthen their cyber defenses.

Combining ML and DL has many benefits. These technologies simplify compliance and risk management, improve fraud detection, and enable advanced threat prevention. They can also improve customer satisfaction by providing proactive security and personalized services.

However, ML and DL implementation is iterative. Continuous monitoring, adaptation, and teamwork are needed to keep up with the rapidly changing threat landscape and technological advances. More research and analysis are needed to determine how these technologies will affect the financial system and consumer confidence.

Bangladesh can improve its financial infrastructure's cybersecurity, protect consumer data, and maintain public confidence in the banking industry by implementing the suggested strategies and focusing on forward-looking initiatives. This ensures a secure digital future for all parties and boosts economic resilience and growth.

References

1. Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. Sensors, 23(15), 6666.
2. Hassan, A. O., Ewuga, S. K., Abdul, A. A., Abrahams, T. O., Oladeinde, M., & Dawodu, S. O. (2024). Cybersecurity in banking: a global perspective with a focus on Nigerian practices. Computer Science & IT Research Journal, 5(1), 41-59.
3. Lewis Jr, A. H. (2023). Cyber realism: a definition of and theory for cyber-based advanced persistent threat (APT) a power dynamic of the fifth domain (Doctoral dissertation, American Public University System).
4. Kafi, M. A., & Akter, N. (2023). Securing financial information in the digital realm: case studies in cybersecurity for accounting data protection. American Journal of Trade and Policy, 10(1), 15-26.
5. Hassan, M., Aziz, L. A. R., & Andriansyah, Y. (2023). The role artificial intelligence in modern banking: an exploration of AI-driven approaches for enhanced fraud prevention, risk management, and regulatory compliance. Reviews of Contemporary Business Analytics, 6(1), 110-132.
6. Sarker, I. H., Khan, A. I., Abushark, Y. B., & Alsolami, F. (2023). Internet of things (iot) security intelligence: a comprehensive overview, machine learning solutions and research directions. Mobile Networks and Applications, 28(1), 296-312.
7. Sarker, I. H. (2023). Multi-aspects AI-based modeling and adversarial learning for cybersecurity intelligence and robustness: A comprehensive overview. Security and Privacy, 6(5), e295.
8. Choithani, T., Chowdhury, A., Patel, S., Patel, P., Patel, D., & Shah, M. (2024). A comprehensive study of artificial intelligence and cybersecurity on Bitcoin, crypto currency and banking system. Annals of Data Science, 11(1), 103-135.
9. Dey, P. K., Chowdhury, S., Abadie, A., Vann Yaroson, E., & Sarkar, S. (2023). Artificial intelligence-driven supply chain resilience in Vietnamese manufacturing small-and medium-sized enterprises. International Journal of Production Research, 1-40
10. Annoni, A., Nativi, S., Çöltekin, A., Desha, C., Eremchenko, E., Gevaert, C. M., ... & Tumampos, S. (2023). Digital earth: yesterday, today, and tomorrow. International Journal of Digital Earth, 16(1), 1022-1072.
11. Kafi, M. A., & Akter, N. (2023). Securing financial information in the digital realm: case studies in cybersecurity for accounting data protection. American Journal of Trade and Policy, 10(1), 15-26.
12. Mızrak, F. (2023). Integrating cybersecurity risk management into strategic management: a comprehensive literature review. Research Journal of Business and Management, 10(3), 98-108.
13. Sarkar, G., & Shukla, S. K. (2023). Behavioral analysis of cybercrime: Paving the way for effective policing strategies. Journal of Economic Criminology, 100034.

doi:10.20944/preprints202409.0645.v1

14. Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking cyber threats: A framework for the future of cybersecurity. Sustainability, 15(18), 13369
15. Hubbard, D. W., & Seiersen, R. (2023). How to measure anything in cybersecurity risk. John Wiley & Sons.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.