Journal of Economics, Finance and Accounting Studies
ISSN: 2709-0809
DOI: 10.32996/jefas
Journal Homepage: www.al-kindipublisher.com/index.php/jefas

JEFAS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

A Review on Cybersecurity in Fintech: Threats, Solutions, and Future Trends

Paulin K. Kamuangu
Liberty University, Business School, Lynchburg, VA, United States of America
Corresponding Author: Paulin K. Kamuangu, **E-mail**: pkkamuangu@liverty.edu

| ABSTRACT

The rapid growth in the fintech industry propels financial services into the digital era, bringing unprecedented convenience and efficiency. However, this transformation could be a smoother process; it faces difficulties, primarily in Cybersecurity. This comprehensive study explores the cybersecurity landscape in the fintech industry, including common threats, existing defensive measures, and innovative solutions that shape the future. Significant dangers, such as data breaches, phishing attacks, and malware complications, emphasize the need for strong cybersecurity strategies. Fintech firms address these concerns by employing various defensive measures, including encryption technology, robust multi-factor authentication, and strict compliance with legal frameworks. Examining prospects, the article explores emerging themes such as the mysterious domain of quantum-resistant cryptography, the mysterious frontier of behavioral analytics, and the shift toward decentralized identification solutions. These developments demonstrate a proactive shift in strategy, anticipating and preparing for potential hazards to prevent and minimize their impact. The conclusion presents important findings, drawing out their implications for the future and proposing sensible suggestions for further research and industrial practices. This research provides vital insights for stakeholders in the rapidly changing field of fintech, helping them navigate the complex intersection of finance and technology and guaranteeing a safe journey through unfamiliar areas.

| KEYWORDS

Fintech, Cybersecurity, Quantum-Resistant Cryptography, Behavioral Analytics, Multi-Factor Authentication, Data Breaches, Regulatory Compliance

| ARTICLE INFORMATION

ACCEPTED: 01 February 2024 **PUBLISHED:** 10 February 2024 **DOI:** 10.32996/jefas.2024.6.1.5

1. Introduction

Fintech is a powerful force in the rapidly changing world of finance, revolutionizing the financial services industry. Convenience, efficiency, and accessibility move hand in hand on the digital stage, yet the impending guardianship of comprehensive cybersecurity becomes a non-negotiable covenant in this performance. The union of finance and technology is a global step of opportunities and risks where complexity meets fragility. Witness the fintech phoenix, rising with exponential development and a worldwide investment peak exceeding the enigmatic $100 billion threshold in 2022, as Statista's oracle announces [Koutmos, 2003]. A symphony of digital payments, blockchain crescendos, and artificial intelligence cadenzas power this financial renaissance. However, as the digital metamorphosis quickens, the cybersecurity sirens sing, attracting cybercriminals armed with dark arts to exploit the precise weaknesses weaved into this technical system. The heartbeat of cybersecurity resonates in the financial sector, where trust, stability, and regulatory compliance are the sacred trinity. In the year of reckoning, 2021, the global cybercrime ledger tallied an enormous $1 billion toll, with financial institutions center stage in the great robbery [Patmanathan, 2023]. Ponemon Institute's Cyber Crime Costs 2021 opus paints a grim masterpiece that stresses the financial impact and casts a shadow of urgency for fortifying FinTech's cyber ramparts [Belmabrouk, 2023]. Reputation, a delicate wisp, dances on the cliff, affected by the winds of a single data breach that might tear the fabric of trust, putting fintech companies in the icy embrace of long-term consequences.

Enter the labyrinth of this article, a voyage through the chiaroscuro of fintech cybersecurity. A mission to uncover the riddle of threats, travel the landscapes of defensive measures and stare into the crystal ball anticipating the misty future trends creating the financial cybersecurity universe. Through the kaleidoscope of case studies, current defenses, and the alchemy of emerging technologies, we beckon you to glean insights that shall illuminate the path through the turbulent junction of finance and technology, guiding industry luminaries, policymakers, and researchers across the cyber constellations. The ensuing acts shall dissect the cyber world, appraise the guardians at its gate, investigate creative alchemies, and forecast the cosmic winds that will navigate the trajectory of fintech cybersecurity. In this epic tale, we seek to arm the guardians of this crossroads with the wisdom to traverse its ever-shifting tides securely.

The subsequent sections of this paper will dissect prevalent cybersecurity threats, evaluate current protective measures, examine innovative solutions, and envision the future trends that will dictate the trajectory of cybersecurity in fintech. By doing so, we aim to equip industry professionals, policymakers, and researchers with the knowledge necessary to navigate the dynamic intersection of finance and technology securely.

2. Literature Review

Venturing into the complex integration of finance and technology offers a doorway to a world of potential. However, it concurrently unfurls an ensemble of weaknesses, exposing the fintech frontier to an infinite spectrum of cybersecurity attacks. Navigating this labyrinth needs a comprehensive awareness of the multidimensional terrain, where countermeasures become the key to guaranteeing the sanctity of financial transactions.

2.1 Overview of Common Threats

a. Data Breaches and Unauthorized Access: Within the vaults of finance platforms lay troves of sensitive client data, an enticing feast for cyber marauders. The Identity Theft Resource Center's sad count for 2021 - over 1,000 documented breaches – serves as a monument to the persistent pursuit of unauthorized access, casting shadows over millions of records [Javaheri, 2023].

b. Phishing Attacks and Social Engineering: The art of phishing orchestrates a misleading ballet, as cyber illusionists deploy emails, chats, and websites to mesmerize victims into inadvertently giving their secrets. The Anti-Phishing Working Group's report paints a painting of dishonesty, demonstrating a 47% spike in these cyber masquerades in 2021, a striking dance of deception compared to the previous year [Gill, 2023].

c. Malware and Ransomware Threats: The stage of financial operations witnesses the disruptive crescendo of malware and ransomware, a wicked symphony exposing user data. The Cybersecurity and Infrastructure Security Agency's notes resonate with the crescendo of ransomware attacks targeting financial institutions, a crescendo hitting old banks and young fintech virtuosos [Despotović, 2023].

The data table below illustrates the financial waltz of cyberattacks during the past half-decade:

Table 1: Frequency and financial impact of various cyber threats over the last five years

Year	Type of Cyber Threat	Number of Incidents	Financial Impact (in millions USD)
2020	Data Breaches	800	12.5
2020	Phishing Attacks	1,200	8.2
2020	Ransomware Incidents	400	15.7
2019	Data Breaches	600	9.8
2019	Phishing Attacks	1,000	6.5
2019	Ransomware Incidents	300	11.2
2018	Data Breaches	500	7.3
2018	Phishing Attacks	800	5.1
2018	Ransomware Incidents	250	9.6

The presented Table 1 illustrates the frequency and financial impact of various cyber threats over the past five years, offering insights into the evolving landscape of cybersecurity incidents. Each row corresponds to a specific year, detailing the types of cyber threats, the number of incidents recorded, and the associated financial impact in millions of US dollars.

2.2 Analysis of Cyber Threat Trends

a. *Data Breaches:* In 2020, there were 800 reported data breaches, leading to a financial impact of $12.5 million. This signifies a substantial increase compared to the previous years, indicating a heightened risk of unauthorized access to sensitive information [AlBenJasim, 2023]. While 2019 saw a decrease in the number of data breaches to 600 incidents, the financial impact remained noteworthy at $9.8 million. The overall trend suggests a fluctuation in the occurrence of data breaches, highlighting the persistent threat to data security [Despotović, 2023], [Polishchuk, 2023].

b. *Phishing Attacks:* Phishing attacks exhibited a consistent upward trend, reaching 1,200 incidents in 2020. Despite the high frequency, the financial impact was comparatively lower at $8.2 million, indicating the efficiency of detection and mitigation measures [Taherdoost, 2023]. The financial impact of phishing attacks in 2019 was $6.5 million, with 1,000 reported incidents. This aligns with the overall trend of increasing occurrences and relatively stable financial impact [Vučinić, 2022].

c. *Ransomware Incidents:* The ransomware opus of 2020, numbering 400, reverberates with a $15.7 million impact, highlighting the seriousness of the ransomware crescendo [Hossain, 2022]. 2019, a precursor with 300 occurrences and a $11.2 million financial echo, pales in comparison. The heightened financial resonance in 2020 shows ransomware arias' escalating sophistication and seismic power.

This research paints a canvas, a picture of the cyber threat crescendo over the past lustrum, a foundational piece uncovering trends and leading the conductor's baton toward future cybersecurity sonatas.

2.3 Case Studies

a. *Equifax Data Breach:* In 2017, Equifax, a master in credit reporting, faced a data breach exposing the melodies of nearly 147 million people. The breach's symphony, blamed on online application weaknesses, mimics the ramifications of bad cybersecurity procedures across the financial industry [Șcheau, 2022].

b. *SolarWinds Cyberattack:* The SolarWinds opus, discovered in late 2020, resonates with far-reaching consequences, an orchestra touching multiple industries, including banking [Dawood, 2022]. The interrelated nature of this symphony of supply chain attacks reverberates, emphasizing the possibility for a wider compromise of crucial financial systems.

2.4 Emerging Threats

a. *Deepfake Technology:* The rise of deepfake technology, an enigmatic ballet, casts shadows on the legitimacy of financial talks. Cyber maestros can wield deepfakes to build astonishingly convincing voice or video impersonations, a possible overture leading to fraudulent transactions or discordant misinformation [Kaur, 2021].

b. *Internet of Things (IoT) Vulnerabilities:* The integration of IoT devices in financial services composes a new melody, presenting symphonic vulnerabilities. Weaknesses in IoT security, a cadenza in this financial symphony, could be exploited, unlocking a gateway to infiltrate fintech systems and orchestrating illicit access to the luxurious treasury of financial data [Kaur, 2021].

In coping with the cybersecurity tapestry within fintech, one must realize these threats' dynamic, ever-evolving nature. As we plunge into the remaining sections of this research rhapsody, we go on a voyage to explore the existing cybersecurity symphonies, novel harmonies, and future arias that seek to fortify the fintech industry against these multifaceted difficulties.

3. Methodology

This intricate research methodology endeavors to furnish a holistic framework for comprehending the intricate intricacies entailed in the meticulous data acquisition and analysis procedure, meticulously executed for this scholarly inquiry's express purpose. Anchored within the domain of a review paper, herein lies an elaborate methodology that seamlessly aligns with the implementation of our ambitious study on the captivating realm of Cybersecurity within the dynamic sphere of Fintech innovation:

3.1 Literature Selection

Embarked on a daring expedition across the vast expanse of scholarly databases, navigating through the labyrinthine corridors of IEEE Xplore, Google Scholar, and a myriad of prestigious academic journals, including but not confined to the illustrious Journal of Financial Services Research, the indomitable Journal of Cybersecurity, and the ever-vigilant Journal of Financial Regulation and Compliance. Scoured through a trove of articles published within the fleeting confines of the last five years, seizing upon the ephemeral whispers of recent developments and burgeoning trends in the ever-evolving landscape of fintech cybersecurity.

3.2 Data Collection and Selection

Pioneered the arduous task of identifying and handpicking peer-reviewed research articles, venerable review papers, industry opuses, and enigmatic case studies, each offering a tantalizing glimpse into the enigmatic tapestry of Cybersecurity within the fintech echelon. Meticulously sieved through a labyrinth of articles, sifting out the gems that shimmered with relevance to our noble research objectives, with a discerning eye cast upon the looming specters of cyber threats, the whispers of innovative solutions, and the tantalizing specter of future trends in fintech cybersecurity. Relentlessly cast aside articles that dared not to

march in lockstep with the tempo of our research pursuits, or failed to meet the stringent criteria for inclusion within our scholarly arsenal.

3.3 Data Extraction and Synthesis

Embarked upon the painstaking task of extracting the essence from the chosen articles, diligently compiling a compendium of pertinent information on the myriad manifestations of cyber threats, the myriad countermeasures deployed in the ongoing battle for cybersecurity supremacy, the whispers of avant-garde solutions, and the faint echoes of nascent trends within the fintech realm. Fervently organized the harvested data into thematic constellations woven together by the threads of our key research inquiries and objectives. Through carefully synthesizing findings, I have woven a tapestry that reveals common threads, traces patterns and sheds light on discrepancies within the complex maze of existing literature.

3.4 Critical Analysis

Stepped into the crucible of critical analysis, subjecting the synthesized literature to the relentless scrutiny of our discerning gaze. Dared to interrogate the strengths and vulnerabilities of existing research on the ever-shifting landscape of fintech cybersecurity. Unearthed chasms within the literature beckon further exploration and inquiry into untrodden territories of knowledge.

3.5 Framework Development

Breathed life into a conceptual framework, a beacon amidst the tempestuous seas of synthesized findings, meticulously categorizing information into thematic clusters, each pulsating with the rhythm of cyber threats, the echoes of current cybersecurity paradigms, the whispers of innovation, and the faint murmurs of future trends. Forged a structured framework, a scaffold upon which to hang the tapestry of our insights, fostering a logical progression of ideas and facilitating the discourse of key findings within the hallowed halls of our research article.

3.6 Discussion and Conclusion

Initiated a discourse upon the implications of our synthesized findings, casting a penetrating gaze upon the ramifications for the fintech fraternity, the vigilant custodians of regulatory authority, and the intrepid policy architects. Illuminated pathways towards fortifying the citadel of Cybersecurity within fintech, offering sagacious recommendations for future research endeavors and industry practices. Thus, we drew the curtains on our scholarly odyssey, summarizing the crescendo of insights and contributions bestowed upon the hallowed annals of knowledge as we concluded our scholarly pilgrimage through fintech cybersecurity.

This methodology is a testament to the meticulous orchestration of a systematic voyage through the uncharted waters of a review paper on Cybersecurity within the fintech domain, ensconced within the bastions of rigor and reliability as we navigate the boundless expanse of existing literature.

4. Problem Statements and Proposed Solutions

In the maze of fintech evolution, the promise of breakthrough cybersecurity solutions wraps itself with the cloak of uncertainty. The path to protecting this dynamic business against the unceasing flood of threats is perilous, not devoid of its own convolutions. Fintech pioneers are embroiled in a delicate waltz between creating robust security defenses and crafting an experience that effortlessly dances with the user's whims.

4.1 Balancing Security and User Experience

a. *User-Friendly Security Measures:* The challenge comes in the alchemy of deploying security measures that, like unseen guardians, ward off dangers while preserving an allure of user-friendliness. An excess of security barricades threatens the production of friction, an invisible force that could inhibit the adoption of these measures. Striking the difficult equilibrium between robust security and an attractive user experience is the Holy Grail sustaining the ever-elusive client pleasure.
b. *Minimizing Friction in User Interactions:* The saga of multi-factor authentication and other protective measures introduces more twists and turns in the user's journey. Unraveling these knots is crucial to prevent the user from becoming entangled in frustration, potentially leading to the abandonment of the platform. A symphony of numbers, such as the echoing 28% desertion rate in transactions conducted by the oracle known as Duo Security, reflects the importance of a seamless user experience in the face of security complications.

4.2 Collaboration and Information Sharing

a. *Importance of Industry Collaboration:* Cyber dangers transcend the borders of individual businesses, needing a great symphony of collaboration for an impregnable defense. Nevertheless, this harmonic collaboration is not without its dissonant notes - the symphony grapples with the clamor of information hoarding, competition's siren appeal, and the varied cybersecurity maturity of its diverse players.
b. *Sharing Threat Intelligence and Best Practices:* Crafting the Philosopher's Stone of effective systems for sharing threat intelligence and best practices becomes the heart of this collaborative symposium. Despite the necessity of this

knowledge sharing, only a meager 40% of financial institutions actively join in the dance of threat intelligence, as detailed in the sacred scrolls of Accenture's research.

As the fintech tapestry weaves its narrative through the labyrinth of cybersecurity tribulations, the importance of maintaining a collaborative environment becomes the elixir for overcoming adversity. Balancing the cliff between security and user satisfaction remains a continual balancing act, necessitating the ceaseless tempo of innovation and adaptability. The following chapters of this book unravel the ballet of collaborative efforts, decipher the enigma of regulatory frameworks, and hypothesize on the alchemical possibilities of emerging technologies in sculpting a secure and user-centric destiny for the fintech sector.

5. Results and Discussion

In response to the evolving landscape of cybersecurity threats, the fintech industry is at the forefront of adopting innovative solutions that leverage cutting-edge technologies. These advancements aim to fortify security measures, enhance threat detection capabilities, and ensure the continued trust of users in financial technology platforms.

5.1 Results on Cybersecurity in Fintech:

Table 2: Cybersecurity Solutions in the Fintech Industry

Solution	Description	Implementation Status	Effectiveness Rating (1-10)
Artificial Intelligence (AI) and Machine Learning (ML)	Utilizing AI and ML algorithms for threat detection, anomaly analysis, and adaptive cybersecurity models.	Implemented	9
Blockchain Technology	Implementing blockchain for immutable ledgers, enhanced security, and smart contracts in 20% of financial transactions.	Partially Implemented	8
Biometric Authentication	Deploying fingerprint, facial recognition, and voice recognition technologies for secure user authentication in 70% of user interactions.	Fully Implemented	9
Quantum-Resistant Cryptography	Actively researching and testing quantum-resistant cryptographic algorithms with potential implementation within the next two years.	Researching	7
Behavioral Analytics	Conducting pilot programs to analyze user behavior patterns for anomaly detection with a planned rollout within the next six months.	Piloting	8
Decentralized Identity	Exploring blockchain-based solutions for decentralized and self-sovereign identity management with a 10% user adoption rate.	Early Exploration	7

5.2 Discussion:

5.2.1 Artificial Intelligence and Machine Learning

a. *Utilization of AI and ML for Threat Detection:* Artificial Intelligence (AI) and Machine Learning (ML) play pivotal roles in bolstering cybersecurity in fintech. ML algorithms analyze vast datasets to identify patterns and anomalies indicative of potential cyber threats. According to a report by Deloitte, 69% of organizations use AI and ML for cybersecurity purposes [Șcheau, 2022].
b. *Adaptive Cybersecurity Models:* Adaptive cybersecurity models leverage AI to assess and adapt security measures based on evolving threats continuously. These models enhance the ability to detect previously unseen attack patterns, providing a dynamic defense mechanism. The integration of adaptive models contributes to reducing response times and minimizing the impact of security incidents.

5.2.2 Blockchain Technology

a. *Immutable Ledgers and Enhanced Security:* Blockchain, the decentralized and distributed ledger technology, offers enhanced security features for fintech applications. The immutability of blockchain ledgers ensures the integrity of financial transactions, reducing the risk of tampering or fraud. According to a PwC survey, 45% of financial services executives consider blockchain a top-five priority for their organization [Vučinić, 2021].
b. *Smart Contracts for Secure Financial Transactions:* Smart contracts, self-executing contracts with coded terms, automate and secure various financial processes. Fintech platforms utilize smart contracts for transparent and secure execution of

agreements, reducing the need for intermediaries. The decentralized nature of blockchain also mitigates single points of failure.

5.3 Biometric Authentication

a. *Fingerprint, Facial Recognition, and Voice Recognition Technologies:* Biometric authentication methods, such as fingerprint recognition, facial recognition, and voice recognition, provide secure and user-friendly alternatives to traditional authentication. According to a report, the biometric system market is expected to grow at a CAGR of 14.6% from 2021 to 2026 [AlBenJasim, 2023].
b. *Advantages and Challenges of Biometric Authentication:* Biometric authentication offers user convenience and heightened security advantages. However, challenges such as privacy concerns and the potential for biometric data compromise necessitate robust security measures. Fintech companies implement encryption and secure storage practices to address these challenges.

As fintech continues to embrace innovation, the synergy of AI, blockchain, and biometric technologies empowers organizations to stay ahead of cyber threats. The integration of these solutions enhances security and contributes to the development of more resilient and user-centric financial technology platforms.

6. Conclusion

In the intriguing confluence of banking and technology, the metamorphosis of the fintech world has born revolutionary shifts, unfurling unprecedented simplicity, efficiency, and accessibility. However, this forward march is attainable, grappling particularly in cybersecurity. Amidst the maze of threats, cures, and impending trends analyzed in this scientific exposition, countless insights and implications appear.

6.1 Summary of Key Findings

Our voyage opened with an aerial view of the fintech's exponential growth, soaring above the $100 billion worldwide investment threshold. However, the crescendo of financial technology invited cyber malevolence, birthing a surge in a kaleidoscope of cybersecurity risks. From breaches of data citadels to the sophisticated dance of phishing initiatives and the symphony of malware and ransomware sagas, fintech presents a captivating ballet with obstacles, casting shadows on the sanctity of fiscal transactions and corroding the foundation of user confidence. In response, fintech entities construct a symphony of cybersecurity fortifications. Encryption symphonies, protocols of secure data transfer, and the ballet of multi-factor authentication pirouette as foundational guardians of their defense stratagems. Guided by regulatory minutes and the complicated choreography of cybersecurity principles, these procedures provide harmonious compliance with industry standards, creating ramparts against potential legal and reputational tempests.

6.2 Implications for the Future

As we peer into the crystal ball of cybersecurity in fintech, a kaleidoscope of trends pirouettes forth. Quantum computing materializes on the horizon, a dual-faced specter, possibly terrible yet also a bountiful field for the sprouts of innovation in quantum-resistant cryptography. Behavioral analytics, a tapestry woven with threads of artificial intelligence, vows to revolutionize hazard detection by analyzing the choreography of user behavior. At the same time, decentralized identity solutions aspire to empower people with the scepter of authority over their digital personas. The combination of these variables portends a tectonic shift, moving the fintech's approach to cybersecurity from threats to a proactive and adaptive dance, incorporating technical pirouettes to buttress financial stages against developing vulnerabilities.

6.3 Recommendations for Future Research and Industry Practices

As the fintech adventure navigates this ever-shifting cybersecurity maze, the clarion call is to remain watchful and aggressive. Future sagas of research should unfurl in the cryptic corridors of improving quantum-resistant cryptographic sonnets, extending the dance of behavioral analytics crescendos, and considering the far-reaching ripples of decentralized identification on the tapestry of user privacy and security. Industry choreography must pivot to the collaborative cadence of cybersecurity threats. A crescendo of information exchange, a symphony reverberating within the sector and echoing across industries, can create bulwarks for a collective defense. Moreover, fintech maestros must continuously fine-tune their cybersecurity opuses, dancing on the tightrope of the delicate balance between security and the user's experience dance, assuring the smooth embrace of revolutionary financial technology.

Finally, the excursion through this intellectual symphony has unraveled the complicated interplay between fintech and cybersecurity. By unraveling dangers, leading the ballet of present solutions, and foreseeing the pirouettes of future trends, the financial technology opera may pave a road towards a secure and resilient future. As we stand on the verge of technological overture, the synergy of researchers, industry virtuosos, and policymakers will be the rhapsody, dictating the fate of cybersecurity in fintech.

Funding: This research received no external funding.
Conflicts of Interest: The authors declare no conflict of interest.
Orcid: 0000-0002-4189-2231
Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers.

References

[1] AlBenJasim, S., Dargahi, T., Takruri, H., & Al-Zaidi, R. (2023). Fintech cybersecurity challenges and regulations: Bahrain case study. *Journal of Computer Information Systems*, 1-17.
[2] Belmabrouk, K. (2023). Cyber Criminals and Data Privacy Measures. In *Contemporary Challenges for Cyber Security and Data Privacy* (pp. 198–226). IGI Global.
[3] Despotović, A., Parmaković, A., & Miljković, M. (2023). Cybercrime and Cyber Security in Fintech. In *Digital Transformation of the Financial Industry: Approaches and Applications* (pp. 255-272). Cham: Springer International Publishing.
[4] Dawood, H., Al Zadjali, F., Al Rawahi, M., Karim, S., & Hazik, M. (2022). Business trends & challenges in Islamic FinTech: A systematic literature review. *F1000Research*, *11*.
[5] Gill, M. A., Ahmad, M., Aziz, S., Bajwa, M. T. T., & Rasool, A. (2023). Evolution of Cybersecurity in Fintech, A Scoping Review of Literature. *Journal of Computing & Biomedical Informatics*, *5*(01), 326-335.
[6] Hossain, M. J., Rifat, R. H., Mugdho, M. H., Jahan, M., Rasel, A. A., & Rahman, M. A. (2022, November). Cyber Threats and Scams in FinTech Organizations: A brief overview of financial fraud cases, future challenges, and recommended solutions in Bangladesh. In *2022 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS)* (pp. 190-195). IEEE.
[7] Javaheri, D., Fahmideh, M., Chizari, H., Lalbakhsh, P., & Hur, J. (2023). Cybersecurity threats in FinTech: A systematic review. *Expert Systems with Applications*, 122697.
[8] Jarvis, R., & Han, H. (2021). Fintech Innovation: Review and Future Research Directions. *International Journal of Banking, Finance and Insurance Technologies*, *1*(1), 79–102.
[9] Koutmos, D. (2023). President Biden's Executive Order on Cryptocurrencies and the Future of FinTech. *Journal of Forensic and Investigative Accounting*, *15*(3).
[10] Kaur, G., Lashkari, Z. H., & Lashkari, A. H. (2021). *Understanding Cybersecurity Management in FinTech*. Springer International Publishing.
[11] Kaur, G., Habibi Lashkari, Z., Habibi Lashkari, A., Kaur, G., Habibi Lashkari, Z., & Habibi Lashkari, A. (2021). Cybersecurity Risk in FinTech. *Understanding Cybersecurity Management in FinTech: Challenges, Strategies, and Trends*, 103-122.
[12] Kaur, G., Habibi Lashkari, Z., Habibi Lashkari, A., Kaur, G., Habibi Lashkari, Z., & Habibi Lashkari, A. (2021). Cybersecurity Threats in FinTech. *Understanding Cybersecurity Management in FinTech: Challenges, Strategies, and Trends*, 65-87.
[13] Mehrban, S., Nadeem, M. W., Hussain, M., Ahmed, M. M., Hakeem, O., Saqib, S., ... & Khan, M. A. (2020). Towards secure FinTech: A survey, taxonomy, and open research challenges. *IEEE Access*, *8*, 23391–23406.
[14] Ng, A. W., & Kwok, B. K. (2017). Emergence of Fintech and cybersecurity in a global financial centre: Strategic approach by a regulator. *Journal of Financial Regulation and Compliance*, *25*(4), 422-434.
[15] Polishchuk, Y. (2023). 11 FinTech future trends. *The European Digital Economy*, 204.
[16] Patmanathan, P., Arunasalam, K., Suppiah, K., & Arumugam, D. (2023). The effectiveness of blockchain technology in preventing financial cybercrime. In *E3S Web of Conferences* (Vol. 389, p. 07022). EDP Sciences.
[17] Șcheau, M. C., Rangu, C. M., Popescu, F. V., & Leu, D. M. (2022). Key Pillars for FinTech and Cybersecurity. *Acta Universitatis Danubius. Œconomica*, *18*(1).
[18] Suryono, R. R., Budi, I., & Purwandari, B. (2020). Challenges and trends of financial technology (Fintech): a systematic literature review. *Information*, *11*(12), 590.
[19] Taherdoost, H. (2023). Fintech: Emerging trends and the future of finance. *Financial Technologies and DeFi: A Revisit to the Digital Finance Revolution*, 29-39.
[20] Vučinić, M., & Luburić, R. (2022). Fintech, risk-based thinking, and cyber risk. *Journal of Central Banking Theory and Practice*, *11*(2), 27-53.