information

MDPI

Review

What Hinders Adoption of Artificial Intelligence for Cybersecurity in the Banking Sector

Adeel Ali * and Mahmood Shah *

Newcastle Business School, University of Northumbria at Newcastle, Newcastle upon Tyne NE1 8ST, UK
* Correspondence: adeel.ali@northumbria.ac.uk (A.A.); mahmood.shah@northumbria.ac.uk (M.S.)

Abstract: AI-enabled cybersecurity systems are becoming common, but their effectiveness is reported to be mixed at best due to some barriers. The primary objective of this systematic literature review is to find barriers associated with the use of AI-enabled cybersecurity systems. A comprehensive systematic literature review approach was implemented in this study. Literature sampled from different databases (Scopus and WOS) was synthesised to synthesise barriers associated with using an AI-enabled cybersecurity system, and a total of 41 papers were selected using systematic inclusion criteria. The study identified several barriers, such as the complexity of systems, lack of top management support, lack of AI-proficient employees, and lack of regulatory support for AI. These barriers are classified into technological, organisational, and environmental. This paper is unique as it focuses on the barriers associated with using advanced technologies such as AI-enabled expert systems for cybersecurity. Thus, the current research makes a novel contribution, arguing that attention is required toward organisational-level issues to protect the system from cyberattacks. This will establish the way for researchers to evaluate these barriers, opening new avenues for empirical research and for practitioners to utilise these systems more effectively.

Keywords: advanced technologies; artificial intelligence; cybersecurity; barriers and banking

check for updates

Citation: Ali, A.; Shah, M. What Hinders Adoption of Artificial Intelligence for Cybersecurity in the Banking Sector. *Information* **2024**, *15*, 760. https://doi.org/10.3390/info15120760

Academic Editors: Dongil Shin and Dongkyoo Shin

Received: 30 October 2024
Revised: 20 November 2024
Accepted: 27 November 2024
Published: 29 November 2024

Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

The amplification of technology use has also shifted banks' perspective on how to operate [1]. Banking and financial institutions have adopted the Internet and related technologies in their operations [1], allowing individuals, institutions, and governments to participate in the modern financial system [2]. Owing to the growing technological footprints, banking systems worldwide have become increasingly vulnerable to cyberattacks.

Due to technological advancements, cyberattacks are becoming increasingly sophisticated [3,4]. The sophisticated nature of these crimes poses a significant challenge to our cyberspace's security and underscores the importance of staying vigilant and proactive in protecting ourselves against such threats [5]. Financial institutions are becoming vulnerable [6]. Cybercriminals regularly target the banking sector for financial gain, causing substantial financial and reputational losses to financial institutions [7].

The impact of cyberattacks can be minimised by detection in the early stages [8]. The literature suggests that organisations already use advanced technologies for several tasks to improve their operations [9–13]. Similarly, AI is also becoming predominant in cyberattack mitigation [14].

By embedding AI in the system, machines can perform tasks more promptly and efficiently than humans [15]. AI-enabled systems can offer improved cyberattack protection compared to traditional tools [16]. Although there is no consensus on the subcategorisation, researchers use AI as an umbrella term for several computation strategies, such as machine learning, deep learning, and other learning techniques [17]. Hence, AI or advanced technologies term is used throughout the article for these technologies.

These advanced technologies are considered a potential solution for cyberattacks, and different AI techniques can be used in cybersecurity for breach prediction, intrusion detection, incident response, and prevention [18,19]. AI can prevent cyberattacks in real time [20] and detect and prevent fraud [18].

The literature indicates that the banking sector requires a state-of-the-art AI-based protection system to help organisations tackle cybersecurity issues. The role of AI is well acknowledged, but the concerns associated with adopting AI in systems are not answered [21]. Reports on the barriers or challenges associated with using AI, ML, and other technologies under the AI umbrella are scattered in the literature.

The application of AI, ML, and other technologies under the umbrella of AI is promising for enhancing cybersecurity. Banks can enhance cybersecurity by using these advanced technologies; however, it is essential to address the associated challenges for their successful implementation [22].

Hence, this current systematic literature review aims to accumulate these barriers while identifying the research streams in the literature. This study can establish the way for future researchers to empirically evaluate these barriers and effectively use these technologies for cybersecurity. This gives the premises to investigate the current research questions, which are:

RQ1: What technological barriers are associated with introducing AI and related technologies for cybersecurity in banking?

RQ2: What organisational barriers are associated with introducing AI and related technologies for cybersecurity in banking?

RQ3: What external barriers are associated with introducing AI and related technologies for cybersecurity in banking?

RQ4: What research streams in the literature contribute to using AI and related technologies for cybersecurity in the banking sector?

RQ5: What are the gaps in the literature?

2. Materials and Methods

2.1. Methodology

The study aimed to synthesise studies investigating barriers and challenges hindering the integration of artificial intelligence in cybersecurity systems. To investigate prior literature, SLR is a promising approach [23]. Hence, this study uses a systematic literature review method with a PRISMA approach to address all elements of using advanced technologies for cybersecurity in banking. First, it is crucial to search for relevant literature and, second, to analyse these studies.

This study includes the Web of Science and Scopus databases. However, for using the snow-bowling technique to find more relevant research, Google Scholar was also searched for forward and reverse snow-bowling to ensure their entirety was correct. The use of advanced technologies like AI and machine learning has recently increased, and many researchers have explored using these technologies to enhance cybersecurity [24]. Hence, the search used in the literature review is limited to publication year from 2018 to 2023. This filtered research outcome is more dependable and representative [25]. The inclusion criteria were keywords, publication year, databases, and peer-reviewed publications.

Keywords were developed to identify the relevant studies in selected databases. Initially, Google Scholar was searched for words like artificial intelligence, cybersecurity, and barriers. After retrieving the initial list of keywords, a panel of fellow researchers and academicians working on cybersecurity issues was formed to select the most relevant keywords. Table A1 presents the selected keywords in Appendix A.

2.2. Research Strings

The study used four research strings in both databases to widen the search for relevant research articles. Research strings were developed to search Scopus and the Web of Science. These databases were searched with similar research strings in two time periods. The first

was in July 2023, and the second string was initiated in December 2023 while limiting the search results between 2018 and 2023 in the first string and the results to 2023 in the second string. These research strings are presented in Table 1.

Table 1. Research strings used to identify literature.

Sr. No.	Strings
1	(TITLE-ABS-KEY (artificial AND intelligence) AND TITLE-ABS-KEY (cybersecurity))
2	(TITLE-ABS-KEY (advanced AND technology) AND TITLE-ABS-KEY (data AND security) AND TITLE-ABS-KEY (theft))
3	(TITLE-ABS-KEY (artificial AND intelligence) AND TITLE-ABS-KEY (bank*))
4	(TITLE-ABS-KEY (machine AND learning) AND TITLE-ABS-KEY (cybersecurity))

In the first stage, these four research strings resulted in 9799 articles from two databases and 3454 results in the second phase, for a total of 13,253.

2.3. Screening Process

The first step was to retrieve the search results from these two databases. The study used Endnote 20 software for this process. The RIS files were downloaded and added to Endnote 20 to retrieve the results for the screening process. In the first stage, using the find duplicate option in Endnote 20, 4221 duplicates were removed. Similarly, sorting articles using the same software removed the book chapters and conference papers. However, the conference titles were checked carefully before being removed to include any relevant study.

This search strategy added seven relevant conference papers to the study. After removing irrelevant conference articles, retracted articles and book chapters, the results were reduced to 6057. In the second phase, the remaining research articles were searched in Endnote 20 with keywords like challenges, barriers, factors, issues, adoption and implementation.

This categorisation strategy reduced the collection relevant to the study's objectives. However, to eliminate the chance of removing any relevant study, the titles and abstracts of the remaining articles were also checked, reducing the results to 689.

In the third stage, 24 articles were removed due to access restrictions, while the remaining articles were accessed. In the final stage, all remaining research articles were accessed for relevance, i.e., relevance to the banking industry and discussion of adoption challenges and barriers, reducing the final results to 41. Figure 1 presents the graphical representation of the whole process.

2.4. Eligibility Criteria

The study developed inclusion and exclusion criteria to achieve the research objectives. The articles were evaluated under these criteria to include the relevant studies in the literature review. The inclusion and exclusion criteria are described in Table 2.

Table 2. Inclusion and exclusion criteria.

Inclusion Criteria	Exclusion Criteria
Articles are published in peer-reviewed journals and reputed conferences	Book chapters and lectures
The study uses artificial intelligence, machine learning, and other technologies under the AI umbrella for cybersecurity	AI, ML, and other relevant technologies not used
Articles discussing the adoption of AI in the banking or financial industry	Banking or financial industry not discussed for use of technology
The study discusses barriers, challenges, and issues while adopting or developing the technology	The challenges, barriers, and issues not discussed

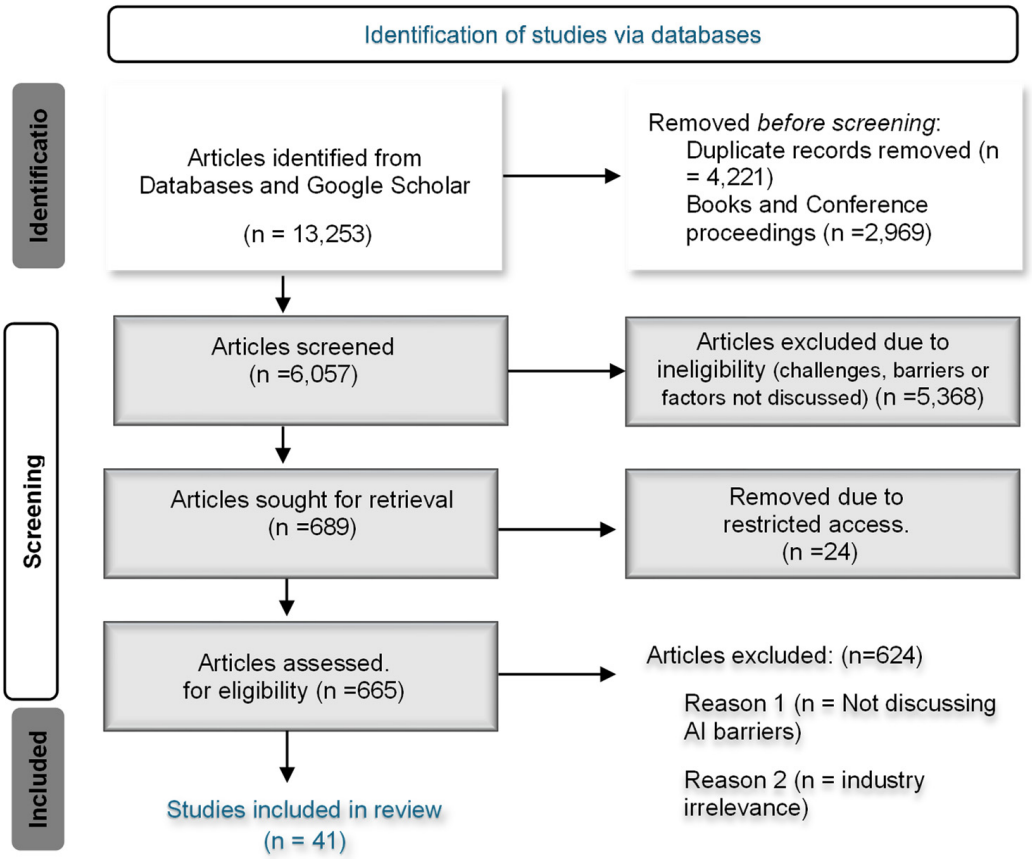

Figure 1. PRISMA flow diagram presenting the selection process of articles.

2.5. TOE Framework

To find and categorise these barriers, the study used the Technology–Organisation–Environment framework. It is considered more explanatory in technology adoption studies [26]. The TOE framework is determined as an appropriate theoretical foundation for the current study as it comprises all the bank dimensions [27]. The TOE framework categorises the technology adoption determinants into three categories, which include technological (i.e., complexity, compatibility, and other factors relating to technology), organisational (i.e., size, management, and employee-related issues), and environmental (i.e., market, government, competition, and other external factors) [28].

3. Results

The general characteristics of the studies in Figure 2 present the number of publications compared to the year of publication.

The literature shows that multiple studies are available on artificial intelligence, machine learning, cybercrime, cybersecurity, and the banking sector. In the research of information systems, researchers have recently started to examine the organisational readiness for AI and other technologies for cybersecurity, such as AL-Dosari, Fetais [29] and Pumplun, Tauchert [30]. However, the research on challenges and barriers associated with the use of these advanced technologies is scattered in the literature. Hence, the current research contributes to the literature in the context of accumulating the barrier suggested by several researchers in one study.

The use of artificial intelligence is increasingly accepted these days in various industries. Industries like telecom, health, hospitality, manufacturing, and finance are a few to mention [31–38]. However, to our knowledge, no study has been found in the literature that has accumulated the barriers associated with using AI, ML, and other advanced cyber-

security technologies in banking or the financial sector. Hence, the current study organises these barriers into the sections that follow.

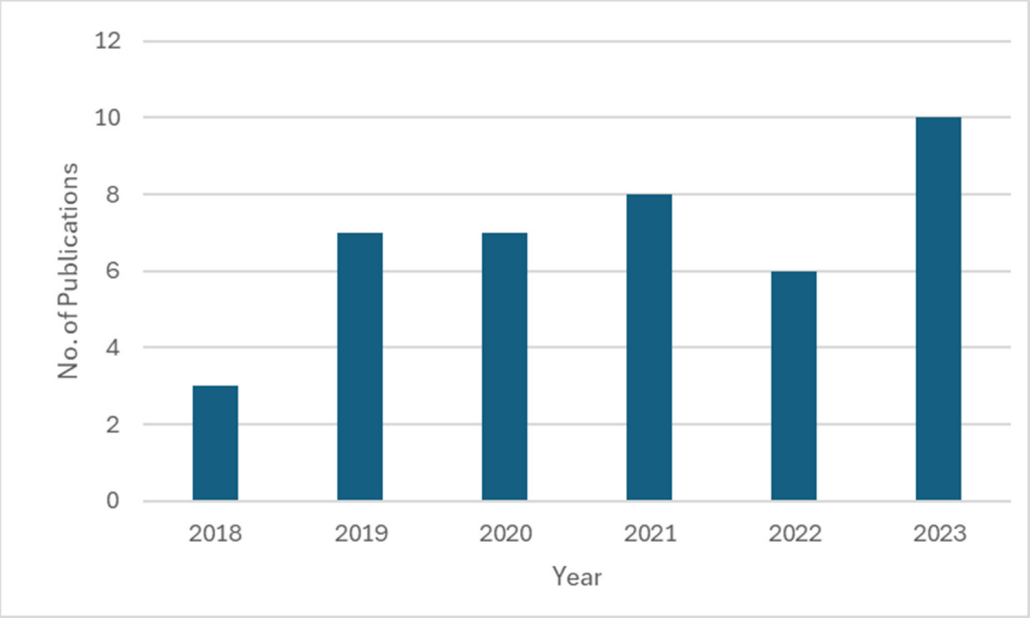

Figure 2. Number of articles published each year.

3.1. Technological Barriers

Technological aspects are essential for the introduction of advanced technology in any organisation. Technology readiness refers to the ability of an organisation to adopt new technology [37]. It can be asserted that technological barriers have a noteworthy influence on implementing advanced technology. Table 3 presents technological barriers associated with the use of advanced technology for cybersecurity.

Table 3. Technological barriers associated with advanced technology use for cybersecurity.

Sr. No.	Barrier	Definition	Reference
1	Compatibility	In terms of integration with the existing infrastructure.	[27,29,30,38–43]
2	Complexity	In terms of the use and maintenance of advanced technology.	[14,27,41]
3	Data Unavailability	The data required by advanced technology to work correctly and produce accurate results.	[30,44–48]
4	Lack of Quality Data	Advanced technology will produce results based on the data provided. Hence, quality data will provide better results.	[27,30,45,49–51]
5	Data Protection	The data used by advanced technology can be vulnerable to attacks.	[30,47,52]

Source: author generated.

The existing literature suggests that the infrastructure may hinder the adoption of advanced cybersecurity technologies. Researchers emphasise that to use AI, a state-of-the-art system is required to handle AI [53]. Similarly, implementing new security features may be limited by outdated and incompatible infrastructure in the domain of AI use for cybersecurity [29,42]. On the contrary, Senyo, Effah [54] have reported an insignificant correlation between new technology and compatibility in developing nations. Similarly, Beatty, Shim [55] contend that the inability to utilise technology does not significantly influence technology adoption. Hence, it is imperative to scrutinise the association amid artificial intelligence (AI)-grounded cybersecurity systems and their suitability within the framework of emerging economies.

The second most prominent barrier identified from the literature for introducing advanced technologies in systems for cybersecurity is the complexity of technology. The literature suggests that introducing new technology can be significantly influenced by the complexity of the relevant technology [56–58]. Thowfeek, Samsudeen [27] and Soni [14] suggest that complexity hinders the implementation of artificial intelligence in systems. On the contrary, Beatty, Shim [55] have reported an insignificant correlation between complexity and the introduction of advanced technology. Hence, it is pertinent to investigate the relationship between complexity and AI technology while using it for cybersecurity.

Artificial intelligence requires extensive data to perform effectively and make decisions. Data reliability depends upon the quality and quantity of data available to AI [30]. Researchers emphasised three data-related issues regarding AI: availability, quality, and data protection [27,30,47]. AI can produce distinctive advantages with valuable data [59]. However, lacking quality data hinders AI adoption [51]. Nicholls, Kuppa [46] suggest that it is challenging for ML systems to decide based on incomplete data. Ransbotham, Kiron [60] argue that various aspects of data are significant barriers to AI while producing mixed results in their study. Arguing that data protection is the uppermost barrier for pioneers of AI users, it is of least concern for experimenters. Protecting these data is also essential, as data are very valuable in today's technologically advanced world [61]. Along with technology-related barriers, organisations may also face internal issues in implementing advanced technology, which can be called organisational barriers.

3.2. Organisational Barriers

The use of advanced technology in the system is an organisation-level decision. It involves investment and capabilities, which is a corporate decision. Top management engages in these decisions. The literature suggests that CEOs and CIOs can accelerate or decelerate new technology adoption processes [28]. Hence, it is pertinent to investigate the organisational aspects of advanced technologies. As shown in Table 4, this review has identified various organisation-related barriers to advanced technology.

Table 4. Organisational barriers associated with advanced technology use for cybersecurity.

Sr. No.	Barrier	Definition	Reference
1	Lack of Top Management Support	Encouragement and understanding of top management regarding advanced technologies.	[27,30,42,51]
2	Conservative Culture	The culture of the organisation encourages employees to use advanced technologies.	[30,38]
3	Lack of Resources	Allocation of resources or a part of revenue for technology improvement and upgradation.	[30,38,42,48,51,52,62]
4	Lack of Knowledge	Knowledge of employees in the organisation regarding advanced technologies.	[38,62–64]
5	Lack of AI-Proficient Employees	Skills of existing employees to use advanced technologies.	[27,29,40,42,43,51,65]
6	Employee Influence and Fear of Change	Resistance from employees in the implementation of advanced technologies in the system.	[11,42,65–67]
7	Industrial Requirements	Requirement of organisation regarding technology.	[30,43]
8	Size of Organisation	The bigger the organisation's size, the more resources to spare for technology adoption.	[30]

Source: author generated.

The most crucial barrier discussed from the organisational perspective can be top management support and influence. Top management influences organisational decisions and strategy [68]. Various research studies found a significant relationship between top management and technology use [42,69,70]. Similarly, studies by Thowfeek, Samsudeen [27] and Pumplun, Tauchert [30] identified the same barrier to artificial intelligence use in organisa-

tions. Top management can also influence organisational culture, which can influence the adoption of advanced technology.

Organisational culture may play an essential role in the success of an organisation. Management shapes this culture and is identified as an essential factor for adoption [71]. Pumplun, Tauchert [30] suggested that organisational culture influences AI adoption. Lai and Guynes [72] suggested no significant relationship exists between encouraging change and technology adoption. With these contradicting results in the literature, this study suggests including conservative culture as a barrier.

The introduction of advanced technologies in the system involves excessive cost. Possession of resources affects capability [73]. Implementing new technology is determined by the financial resources allocated in the budget [30]. Researchers have found the relationship between cost and new technology implementation significant [62,74]. Hence, this study suggests investigating and includes lack of resources as a barrier to advanced technology-enabled cybersecurity systems.

Another variable identified in the literature as a barrier is the lack of knowledge of technology. It is pertinent to mention the study reported in [64], which used a survey design using 302 employees of the banking sector of Pakistan to check the impact of cybercrime on the performance of an organisation with moderation of information security awareness. The study suggested that cybercrime is negatively associated with the organisation's performance, but this negative impact can be reduced with the help of awareness about information security. Hence, knowledge regarding cybercrime and awareness programs can help reduce these issues. This may also encourage employees to improve their skills regarding the use of advanced technology.

Lack of skills and absence of AI-proficient employees are suggested to be barriers to advanced technology implementation by several researchers [27,40,42]. AL-Dosari, Fetais [29] identified a lack of skills as a barrier to AI use in cybersecurity. Researchers found a significant relationship between knowledge and AI adoption [42]. This lack of skills can create a fear of change in existing employees, which may result in resistance to advanced technology.

Employees may influence organisational decisions. Rodrigues, Ferreira [66] suggest that employees have the most influence over all aspects, such as innovation, consumer, political–legal factors, and internal bank management. Öztürk and Kula [67] suggest that banks use AI for several processes, which may result in employee job losses. However, Nam, Dutt [33] argue that employees would not resist using artificial intelligence in the system.

Specification of one industry can differ from another, affecting the adoption of AI-enabled systems [30]. Hence, the industrial requirement variable is essential in using advanced technologies for cybersecurity. Depending on the nature, industry-specific properties can positively or negatively influence an organisation's adoption of advanced technologies [30]. As every industry has different requirements, it is necessary to investigate whether it affects the use of advanced technology for cybersecurity systems.

Last but not least, size is another prominent variable reported in the literature. Various researchers in the literature have found a significant relationship between the size of an organisation and technology adoption [30,75,76].

3.3. Environmental Barriers

Environmental aspects comprise external factors that influence an organisation's decisions and strategies. When using advanced technology, these external environmental factors can include the government and competitors. Hence, these factors are included in the study and presented in Table 5.

Table 5. Environmental barriers associated with advanced technology use in cybersecurity.

Sr. No.	Barrier	Definition	Reference
1	Regulatory Issues	It can be categorised as support from the government.	[27,29,40,42,47,77,78]
2	Legal Issues	Legal issues associated with regulatory frameworks and data use.	[47,48]
3	Privacy and Ethical	Privacy and ethical issues related to the use of customers' data for advanced technology	[27,43,48,51,62,79–82]
4	Lack of Competitor Pressure	Use of advanced technologies by competitors.	[30]
5	Consumer Readiness	Readiness of end-user.	[10,12,13,30,42,83–85]

Source: author generated.

As both victims and perpetrators of crime can use artificial intelligence, policies and regulations are needed to help organisations accelerate the use of advanced cybersecurity technologies. Although developing countries enact legislation and provide a framework, these regulations are still very basic and can be manipulated easily [86]. Abidin, Nawawi [77] discovered that the policy to protect customer data exists, but data breaches are still happening because of employees' attitude of ignoring company policies. These issues may be mitigated with strict compliance. Developing countries must bring their anti-cybercrime policies to international standards [87]. Several researchers have identified a lack of regulatory framework, regulatory requirements, and lack of regulatory support as barriers to technology used in industry [27,29,40].

Due to the unavailability or immaturity of the regulatory framework, legal issues may also arise for organisations. These frameworks need improvements [88]. Wang, Nnaji [89] conducted their research on 17 banks and 27 banking security companies with an online survey, targeting employees who engage in information security operations. The study observed that the Nigerian banking industry is aware of traditional cybercrime but is struggling with technologically advanced cybercrime. The study suggests that an integrated approach is required to address these issues. Also, both technological and legal advancements are required.

Similarly, several researchers identified that data privacy and ethical issues could affect advanced cybersecurity systems [62,79,80]. Kjamilji, Savaş [48] suggest that AI-enabled systems can be trained better by combining data from different organisations. However, no organisation is willing to share data due to legal and privacy issues. Taddeo [79] suggests that there are ethical issues associated with the deployment of AI in cybersecurity, and these issues may overcome the benefits associated with AI. Hence, these issues are to be addressed before using AI in cybersecurity. Sarma, Matheus [90] suggested that ethical and legal issues must be addressed to obtain the full potential of AI in cybersecurity.

Competition is like a booster for organisations. The threat of losing a competitive advantage may be a catalyst in implementing advanced technology. If the competition for adopting advanced technology is absent in the industry, the organisations may not evolve or use advanced technology. While competition is crucial, end users or consumers are essential to any organisation.

Any organisation needs to assess what consumers' approach is regarding technology adoption. Several researchers have accessed customer satisfaction and readiness for AI adoption. Ali, Swiety [13] and Alandikar and Prabhu [10] suggest that from the customers' point of view, AI-led banking is providing better customer services. Similarly, Lee and Chen [84] suggest that using AI increases customers' willingness to adopt mobile banking. Hence, customer resistance can also be a barrier to adopting advanced technologies.

The aforementioned studies in the literature suggest that advanced technology can enhance security by detecting and preventing in real-time, which can enhance bank processes and customer satisfaction [29,40,62,91]. Advanced technologies have multiple uses in the banking sector. However, to adopt these advanced technologies on a full scale, issues like lack of infrastructure, data privacy, resources, knowledge, and regulatory compliance

should be addressed to gain the trust of all stakeholders. These issues can only be resolved when all stakeholders, in particular government, clients, employees, and top management, are in agreement to form policies and regulations.

4. Research Streams and Gaps in Literature

The literature synthesis identified four research streams in the literature. Various researchers have contributed to the literature in the domain of advanced technology and cybersecurity. The initial debate in this domain was on technical issues, which are still relevant. Issues like algorithm development and system development for cybersecurity were the focus. Donepudi [92] analysed various advanced techniques for cybersecurity in his research by pointing out associated issues and providing advanced solutions. Patil [93] performed a literature review on AI use for cybersecurity and suggested that we can improve the cybersecurity capability of artificial intelligence with a better understanding and handling of data in machine learning. Mohammed [94] performed a literature review to analyse how AI works in cybersecurity and pointed out several technical issues. The literature suggests that these issues are still present and emphasised by researchers.

Afterward, as presented in Figure 3, the focus shifted toward positive and negative use of these advanced technologies. For instance, these technologies can be used by both attacker and victim. Raban and Hauptman [81] evaluated the positives and negatives of emerging technologies. Yeoh [80] assessed AI's positive and negative aspects for financial crime.

Figure 3. Four research streams in the literature.

Similarly, the third shift in the literature is toward ethical and legal issues associated with using AI for cybersecurity. Taddeo [79] identified three ethical issues associated with AI use in cybersecurity. Presently, the research shift is toward organisational and individual hurdles in deploying advanced cybersecurity technology. Many researchers addressed individual issues with empirical studies [40,62,67,69]. Limited literature is available on organisational-level issues.

After an extensive literature review, only two studies address this issue on an organisational level. The study initiated by [27] followed an interview-based study that lacked empirical testing. Similarly, the study looks at the usual use of AI in banking. The second study in the literature initiated by [29] followed the qualitative method. The study's holistic approach does not focus on barriers associated with AI-enabled cybersecurity systems.

The research on organisational readiness has recently started. Most of the research revolves around the development of the system and its requirements, i.e., technical aspects. Researchers have contributed to individual aspects; however, barriers associated with individuals in cybersecurity are partially discussed. This literature review suggests that most research is on adopting advanced technologies in different organisation departments. These include customer and organisation employee-level studies [9–11,13,27,95].

Although the current shift is toward organisational readiness, researchers are more focused on the factors that can help the adoption of AI in organisations. The challenges that

can arise from the integration are still partially discussed. Similarly, the research has not found any study explicitly focused on the barriers or challenges associated with using AI and other advanced technologies for cybersecurity. The gaps in the literature are mentioned in Table 6.

Table 6. Gaps in literature.

Gap	Detail
Focus on the development of the system	Most of the literature focuses on the development of AI and related solutions
Scattered literature on barriers	The studies mention barriers as a byproduct of the study, mentioned on the sidelines.
Mitigation of barriers	The solution to challenges associated with adopting these technologies is not provided.

Source: author generated.

5. Discussion and Future Directions

The current study attempts to organise and accumulate barriers associated with using AI, ML, and related technologies for cybersecurity in the banking sector. The study formulated four research questions to find and mould these barriers in the TOE framework. These questions are revisited in the following paragraphs.

RQ1. *What technological barriers are associated with introducing AI and related technologies for cybersecurity in banking?*

The technological barriers associated with the use of AI and related technologies are complexity and data-related issues. The existing systems in the banking industry comprise legacy systems, which makes integration of new technology difficult. Another issue arising from the adoption is the complexity of the developed system, making it difficult to operate and maintain systems. Similarly, while developing and training advanced technologies for cybersecurity, researchers require data. Data-related issues such as availability, quality, and data protection are challenges.

RQ2. *What organisational barriers are associated with introducing AI and related technologies for cybersecurity in banking?*

The organisational barriers associated with the use of advanced technology are presented in Table 4. Barriers include top management support, culture, resources, employee-related issues, requirements, and size. Top management is the decision-maker in the organisation. However, the most prominent barriers identified by the researchers are a lack of resources and AI-proficient employees.

RQ3. *What external barriers are associated with introducing AI and related technologies for cybersecurity in banking?*

The environmental barriers associated with the use of advanced technologies are presented in Table 5. The current literature review has identified external barriers such as regulatory, legal, privacy, ethics, lack of competition, and consumer readiness, thus answering the third research question. The most prominent barriers identified in the literature are regulatory, privacy, and ethical issues.

RQ4. *What research streams in the literature contribute to using AI and related technologies for cybersecurity in the banking sector?*

Figure 3 presents the research streams in the literature. The current systematic literature review identified four main research streams. The first research stream is developing

new cybersecurity techniques, data, and integration issues. After developing these systems, the second research stream revolves around the ethical and legal aspects of these systems, such as the ethical use of data, protection of data, and following the legal framework, which currently require improvements. The third research stream in the literature is about the individual aspects. To use these systems, individuals must accept them and undergo training to operate them. The final research stream is very recent and revolves around organisational readiness.

RQ5. *What are the gaps in the literature?*

The final and essential research question was regarding the gaps in the literature. The identified research gaps in the literature are presented in Table 6. The literature review suggests that the development stage is of the utmost importance out of all research streams. Similarly, another gap found is that the literature on barriers is scattered; hence, the current study assembled these barriers and presented them using the TOE framework, which is highly used in IS research. Finally, there is a lack of research on mitigation strategies to overcome these barriers.

5.1. Potential Solutions for Barriers

5.1.1. Upgrading Existing Legacy Systems

The technological barriers to adopting AI-enabled cybersecurity solutions can be mitigated by continuously upgrading existing legacy systems in organisations. The barriers identified in this systematic literature review are related to integrating and training the systems. The data required for the training are captured from the existing system. Hence, improving legacy systems and increasing the computing power of existing systems can resolve a few technology-related issues. The transformation can improve processes, and digital transformation is a part of current global policy [96]. The techniques under the umbrella of AI learn from data, and these developed techniques acquire data through integration with existing systems. Henceforth, integration and other data-related issues can be resolved with existing ecosystem advancements.

5.1.2. Initiative by Top Management

Top-to-bottom initiatives in an organisation are considered to face less resistance. The barriers identified in the literature are related to strategy or individuals in an organisation. Organisations can mitigate or reduce these barriers with the influence of top management [97]. The top management can provide support by providing resources, training, monitoring, and coaching to employees for easy transition [98]. The top management has the authority to influence strategy and allocate resources for adopting technology; hence, it is highly unlikely to adopt a technology when top management is not supportive [99].

5.1.3. Government and Regulator Influence

The banking sector is a highly regulated industry [100]. These regulations also affect the governance systems [101], which can ultimately affect the decisions on the adoption of technology. Hence, the role of government and regulators is essential for these technologies. The regulator should develop strategies that encourage the use of advanced technology. The external or environmental barriers to adopting advanced technologies can be reduced or mitigated with government providing encouragement and a clear framework on the use of advanced technologies.

5.2. Future Recommendation

The use of AI is different for every case [102]. Barriers to AI use in every case can also be different. Hence, studying and evaluating these barriers is pertinent to establish the way for AI use. The current study of the literature has identified several gaps.

The current study has identified various barriers to the adoption of advanced technology. To validate these findings empirically, these identified barriers from the literature can be used to develop a framework based on the TOE framework.

6. Conclusions

With the increase in technology use, cyberattacks are a growing concern, especially in developing countries. As advanced technology provides a real-time solution to these attacks, using advanced technology to tackle cybercrimes is inevitable.

The literature suggests multiple uses of advanced technology in the banking sector, such as chatbots, AI-integrated mobile apps, data mining, providing tailored solutions to customers, anti-money laundering solutions, stopping terror financing, and real-time detection of cyberthreats. Also, it is found that banks are facing issues of data breaches and other cyberattacks, which advanced technologies can mitigate.

However, there are barriers to using advanced technologies in the banking sector, which were mentioned in the literature, such as regulatory issues, employee resistance, lack of skills, compatibility of existing systems, and poor support from top management.

The study examines the barriers to using advanced technologies like AI, ML, and others. The findings reveal that organisations are facing barriers internally and externally. However, the research on barriers is scattered in the literature, and more attention is being directed toward developing new techniques.

This research suggests that organisations should address these issues to safeguard customers and organisations from cyberattacks. Training and knowledge can reduce issues for existing employees. As banks make huge profits, they should invest in IT infrastructure to establish the way for advanced technology-enabled machines, which the literature suggests improve organisational performance. Issues about regulatory authorities regarding the development of regulations and policies should be settled by taking all stakeholders on board for sustainable implementation of advanced technologies for cybersecurity.

Few studies in the literature have tried to address this issue. An integrated approach must address the barriers to implementing advanced technology in cybersecurity.

Author Contributions: Conceptualization: A.A.; methodology, A.A.; software, A.A.; validation, A.A.; investigation, A.A.; data curation, A.A.; writing—original draft preparation, A.A.; writing—review and editing, A.A. & M.S.; visualization, A.A.; supervision, M.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

Table A1. List of key words and databases.

S. No	List of Key Words	List of Databases
1	Artificial Intelligence	Web of Science
2	Machine Learning	Scopus
3	Bank *	Google Scholar (Search engine)
4	Advanced technology	
5	Cybersecurity	
6	Data security	
7	Theft	

* An asterisk is used in research strings to capture all word variations.

References

1. Balkan, B. *Impacts of Digitalization on Banks and Banking. The Impact of Artificial Intelligence on Governance, Economics and Finance*; Bozkuş Kahyaoğlu, S., Ed.; Springer Nature: Singapore, 2021; Volume 1, pp. 33–50. [CrossRef]
2. Khan, S.; Rabbani, M.R. Chatbot as Islamic Finance Expert (CaIFE) When Finance Meets Artificial Intelligence. In Proceedings of the 2020 4th International Symposium on Computer Science and Intelligent Control, Newcastle upon Tyne, UK, 17–19 November 2020; pp. 1–5.
3. Tounsi, W.; Rais, H. A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Comput. Secur.* **2018**, *72*, 212–233. [CrossRef]
4. Guembe, B.; Azeta, A.; Misra, S.; Osamor, V.C.; Fernandez-Sanz, L.; Pospelova, V. The Emerging Threat of Ai-driven Cyber Attacks: A Review. *Appl. Artif. Intell.* **2022**, *36*, 1–34. [CrossRef]
5. Mushtaq, S.; Shah, M. Critical Factors and Practices in Mitigating Cybercrimes within E-Government Services: A Rapid Review on Optimising Public Service Management. *Information* **2024**, *15*, 619. [CrossRef]
6. Islam, U.; Muhammad, A.; Mansoor, R.; Hossain, M.S.; Ahmad, I.; Eldin, E.T.; Khan, J.A.; Rehman, A.U.; Shafiq, M. Detection of Distributed Denial of Service (DDoS) Attacks in IOT Based Monitoring System of Banking Sector Using Machine Learning Models. *Sustainability* **2022**, *14*, 8374. [CrossRef]
7. Hiscox. The Hiscox Cyber Readiness Report 2022. Available online: https://www.hiscox.co.uk/cyberreadiness (accessed on 23 July 2023).
8. Albshaier, L.; Almarri, S.; Rahman, M.M.H. Earlier Decision on Detection of Ransomware Identification: A Comprehensive Systematic Literature Review. *Information* **2024**, *15*, 484. [CrossRef]
9. Ammirato, S.; Sofo, F.; Felicetti, A.M.; Raso, C. The potential of IoT in redesigning the bank branch protection system An Italian case study. *Bus. Process Manag. J.* **2019**, *25*, 1441–1473. [CrossRef]
10. Alandikar, R.; Prabhu, G. A study of digital banking with intervention of artificial intelligence in 21st century. *Shodh Sarita* **2020**, *7*, 155–162.
11. Elegunde, A.F.; Osagie, R. Artificial Intelligence Adoption and Employee Performance in the Nigerian Banking Industry. *Int. J. Manag. Adm.* **2020**, *4*, 189–205. [CrossRef]
12. Yussaivia, A.M.; Lub, C.Y.; Syariefc, M.E.; Suhartantod, D. Millennial Experience with Mobile Banking and Artificial Intelligent (AI)-enabled Mobile Banking: Evidence from Islamic Banking. *Int. J. Appl. Bus. Res.* **2021**, *3*, 39–53. [CrossRef]
13. Ali, M.S.; Swiety, I.A.; Mansour, M.H. Evaluating the Role of Artificial Intelligence in the Automation of the Banking Services Industry: Evidence from Jordan. *Humanit. Soc. Sci. Lett.* **2022**, *10*, 383–393. [CrossRef]
14. Soni, V.D. Role of Artificial Intelligence in Combating Cyber Threats in Banking. *Int. Eng. J. Res. Dev.* **2019**, *4*, 7. [CrossRef]
15. Soni, V.D. Challenges and Solution for Artificial Intelligence in Cybersecurity of the USA. 2020. Available online: https://ssrn.com/abstract=3624487 (accessed on 28 July 2023).
16. Wirkuttis, N.; Klein, H. Artificial intelligence in cybersecurity. *Cyber Intell. Secur.* **2017**, *1*, 103–119.
17. Knoedler, L.; Knoedler, S.; Allam, O.; Remy, K.; Miragall, M.; Safi, A.-F.; Alfertshofer, M.; Pomahac, B.; Kauke-Navarro, M. Application possibilities of artificial intelligence in facial vascularized composite allotransplantation—A narrative review. *Front. Surg.* **2023**, *10*, 1266399. [CrossRef] [PubMed]
18. Narsimha, B.; Raghavendran, C.V.; Rajyalakshmi, P.; Reddy, G.K.; Bhargavi, M.; Naresh, P. Cyber Defense in the Age of Artificial Intelligence and Machine Learning for Financial Fraud Detection Application. *Int. J. Electr. Electron. Res.* **2022**, *10*, 87–92. [CrossRef]
19. Taherdoost, H. Insights into Cybercrime Detection and Response: A Review of Time Factor. *Information* **2024**, *15*, 273. [CrossRef]
20. Creado, Y.; Ramteke, V. Active cyber defence strategies and techniques for banks and financial institutions. *J. Financ. Crime* **2020**, *27*, 771–780. [CrossRef]
21. Raúl, J.V.; Laberiano, A.A.; Pedro, M.V.; Cesar, Y.A. Financial revolution: A systemic analysis of artificial intelligence and machine learning in the banking sector. *Int. J. Electr. Comput. Eng.* **2024**, *14*, 1079–1090. [CrossRef]
22. Babu Nuthalapati, S. AI-Enhanced Detection and Mitigation of Cybersecurity Threats in Digital Banking. *Educ. Adm. Theory Pract.* **2023**, *29*, 357–368. [CrossRef]
23. Borrego, M.; Foster, M.J.; Froyd, J.E. Systematic Literature Reviews in Engineering Education and Other Developing Interdisciplinary Fields. *J. Eng. Educ.* **2014**, *103*, 45–76. [CrossRef]
24. Shukla, A. Leveraging AI and ML for Advance Cyber Security. *J. Artif. Intell. Cloud Comput.* **2022**, *142*, 2–3. [CrossRef]
25. Yang, H.; Tate, M. A descriptive literature review and classification of cloud computing research. *Commun. Assoc. Inf. Sys.* **2012**, *31*, 2. [CrossRef]
26. Oliveira, T.; Martins, M.F. Literature review of information technology adoption models at firm level. *Electron. J. Inf. Syst. Eval.* **2011**, *14*, 110–121.
27. Thowfeek, M.H.; Samsudeen, S.; Sanjeetha, M.B.F. Drivers of artificial intelligence in banking service sectors. *Solid State Technol.* **2020**, *63*, 6400–6411.
28. Al Hadwer, A.; Tavana, M.; Gillis, D.; Rezania, D. A Systematic Review of Organizational Factors Impacting Cloud-based Technology Adoption Using Technology-Organization-Environment Framework. *Internet Things* **2021**, *15*, 100407. [CrossRef]
29. AL-Dosari, K.; Fetais, N.; Kucukvar, M. Artificial Intelligence and Cyber Defense System for Banking Industry: A Qualitative Study of AI Applications and Challenges. *Cybernet Syst.* **2022**, *55*, 1–29. [CrossRef]

30. Pumplun, L.; Tauchert, C.; Heidt, M. A new organizational chassis for artificial intelligence-exploring organizational readiness factors. In Proceedings of the ECIS, Stockholm, Sweden, 8–14 June 2019.
31. Chen, H.; Li, L.; Chen, Y. Explore success factors that impact artificial intelligence adoption on telecom industry in China. *J. Manag. Anal.* **2020**, *8*, 36–68. [CrossRef]
32. Seethamraju, R.; Hecimovic, A. Adoption of artificial intelligence in auditing: An exploratory study. *Aust. J. Manag.* **2022**, *48*, 780–800. [CrossRef]
33. Nam, K.; Dutt, C.S.; Chathoth, P.; Daghfous, A.; Khan, M.S. The adoption of artificial intelligence and robotics in the hotel industry: Prospects and challenges. *Electron. Mark.* **2020**, *31*, 553–574. [CrossRef]
34. Pillai, R.; Sivathanu, B. Adoption of artificial intelligence (AI) for talent acquisition in IT/ITeS organizations. *Benchmarking Int. J.* **2020**, *27*, 2599–2629. [CrossRef]
35. Chatterjee, S.; Rana, N.P.; Dwivedi, Y.K.; Baabdullah, A.M. Understanding AI adoption in manufacturing and production firms using an integrated TAM-TOE model. *Technol. Forecast. Soc. Change* **2021**, *170*, 120880. [CrossRef]
36. Kruse, L.; Wunderlich, N.; Beck, R. Artificial intelligence for the financial services industry: What challenges organizations to succeed. In Proceedings of the 52nd Hawaii International Conference on System Sciences, Grand Wailea, Maui, HI, USA, 8–11 January 2019; pp. 6408–6417.
37. Richey, R.G.; Daugherty, P.J.; Roath, A.S. Firm Technological Readiness and Complementarity: Capabilities Impacting Logistics Service Competency and Performance. *J. Bus. Logist.* **2011**, *28*, 195–228. [CrossRef]
38. Alattas, K. Saudi Arabia Corporate Firms are Hesitant to Embrace Artificial Intelligence as of 2020 Despite the Numerous Benefits. *WSEAS Trans. Syst. Control* **2023**, *18*, 38–46. [CrossRef]
39. Hammadeh, K.; Kavitha, M. Unraveling Ransomware: Detecting Threats with Advanced Machine Learning Algorithms. *Int J Adv. Comput. Sci.* **2023**, *14*, 484–491. [CrossRef]
40. Rahman, M.; Ming, T.H.; Baigh, T.A.; Sarker, M. Adoption of artificial intelligence in banking services: An empirical analysis. *Int. J. Emerg. Mark.* **2023**, *18*, 4270–4300. [CrossRef]
41. Dietz, C.; Dreo, G.; Sperotto, A.; Pras, A. Towards adversarial resilience in proactive detection of botnet domain names by using MTD. In Proceedings of the NOMS 2020-2020 IEEE/IFIP Network Operations and Management Symposium, Budapest, Hungary, 20–24 April 2020; pp. 1–5. [CrossRef]
42. Alsheibani, S.A.; Cheung, D.; Messom, D. Factors inhibiting the adoption of artificial intelligence at organizational-level: A preliminary investigation. In Proceedings of the Twenty-fifth Americas Conference on Information Systems, Cancun, Mexico, 15–17 August 2019. Available online: https://aisel.aisnet.org/amcis2019/adoption_diffusion_IT/adoption_diffusion_IT/2/ (accessed on 28 July 2023).
43. Kruglova, I.A.; Dolbezhkin, V.A. Objective barriers to the implementation of blockchain technology in the financial sector. In Proceedings of the 2018 International Conference on Artificial Intelligence Applications and Innovations (IC-AIAI), Nicosia, Cyprus, 31 October–2 November 2018; pp. 47–50. [CrossRef]
44. Adiban, M.; Siniscalchi, S.M.; Salvi, G. A step-by-step training method for multi generator GANs with application to anomaly detection and cybersecurity. *Neurocomputing* **2023**, *537*, 296–308. [CrossRef]
45. Prasad, A.; Chandra, S. Machine learning to combat cyberattack: A survey of datasets and challenges. *J. Def. Model. Simul.* **2023**, *20*, 577–588. [CrossRef]
46. Nicholls, J.; Kuppa, A.; Le-Khac, N.A. Financial Cybercrime: A Comprehensive Survey of Deep Learning Approaches to Tackle the Evolving Financial Crime Landscape. *IEEE Access* **2021**, *9*, 163965–163986. [CrossRef]
47. Thach, N.N.; Hanh, H.T.; Huy, D.T.N.; Gwozdziewicz, S.; Nga, L.T.V.; Huong, L.T.T.; Nam, V.Q. Technology Quality Management of the Industry 4.0 and Cybersecurity Risk Management on Current Banking Activities in Emerging Markets—The Case in Vietnam. *Int. J. Qual. Res.* **2021**, *15*, 845–856. [CrossRef]
48. Kjamilji, A.; Savaş, E.; Levi, A. Efficient secure building blocks with application to privacy preserving machine learning algorithms. *IEEE Access* **2021**, *9*, 8324–8353. [CrossRef]
49. Chimphlee, S.; Chimphlee, W. Machine learning to improve the performance of anomaly-based network intrusion detection in big data. *Indones. J. Electr. Eng. Comput. Sci.* **2023**, *30*, 1106–1119. [CrossRef]
50. Li, Y.; Wen, G. Research and Practice of Financial Credit Risk Management Based on Federated Learning. *Eng. Lett.* **2023**, *31*, 271–278.
51. Kumari, B.; Kaur, J.; Swami, S. System dynamics approach for adoption of artificial intelligence in finance. In *Advances in Systems Engineering: Select Proceedings of NSC*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 555–575. [CrossRef]
52. Chang, K.; Huang, H. Exploring the management of multi-sectoral cybersecurity information-sharing networks. *Gov. Inf. Q.* **2023**, *40*, 101870. [CrossRef]
53. Maroufkhani, P.; Iranmanesh, M.; Ghobakhloo, M. Determinants of big data analytics adoption in small and medium-sized enterprises (SMEs). *Ind. Manag. Data Syst.* **2023**, *123*, 278–301. [CrossRef]
54. Senyo, P.K.; Effah, J.; Addae, E. Preliminary insight into cloud computing adoption in a developing country. *J. Enterp. Inf. Manag.* **2016**, *29*, 505–524. [CrossRef]
55. Beatty, R.C.; Shim, J.P.; Jones, M.C. Factors influencing corporate web site adoption: A time-based assessment. *Inf. Manag.* **2001**, *38*, 337–354. [CrossRef]

56. Cordery, C.J.; Fowler, C.J.; Mustafa, K. A solution looking for a problem: Factors associated with the non-adoption of XBRL. *Pac. Account. Rev.* **2011**, *23*, 69–88. [CrossRef]
57. Daghfous, A.; Belkhodja, O.; Ahmad, N. Understanding and managing knowledge transfer for customers in IT adoption. *Inf. Technol. People* **2018**, *31*, 428–454. [CrossRef]
58. Hashimy, L.; Jain, G.; Grifell-Tatjé, E. Determinants of blockchain adoption as decentralized business model by Spanish firms–an innovation theory perspective. *Ind. Manag. Data Syst.* **2022**, *123*, 204–228. [CrossRef]
59. Gudigantala, N.; Madhavaram, S.; Bicen, P. An AI decision-making framework for business value maximization. *AI Mag.* **2023**, *44*, 67–84. [CrossRef]
60. Ransbotham, S.; Kiron, D.; Gerbert, P.; Reeves, M. Reshaping Business with Artificial Intelligence: Closing the Gap between Ambition and Action. *MIT Sloan Manag. Rev.* **2017**, *59*, 1532–9194.
61. Dadwal, S.; Haq, A.; Jamal, A.; Nawaz, I. Value of data as a currency and a marketing tool. In *Strategy, Leadership, and AI in the Cyber Ecosystem*; Elsevier: Amsterdam, The Netherlands, 2021; pp. 381–398. [CrossRef]
62. Shambira, L. Exploring the Adoption of Artificial Intelligence in the Zimbabwe Banking Sector. *Eur. J. Soc. Sci. Stud.* **2020**, *5*, 1–15. [CrossRef]
63. Bukht, T.F.N.; Raza, M.A.; Awan, J.H.; Ahmad, R. Analyzing cyber-attacks targeted on the Banks of Pakistan and their Solutions. *Int. J. Comput. Sci. Net.* **2020**, *20*, 31–38.
64. Malik, M.S.; Islam, U. Cybercrime: An emerging threat to the banking sector of Pakistan. *J. Financ. Crime* **2019**, *26*, 50–60. [CrossRef]
65. Almansour, M. Artificial intelligence and resource optimization: A study of Fintech start-ups. *Resour. Policy* **2023**, *80*, 103250. [CrossRef]
66. Rodrigues, A.R.D.; Ferreira, F.A.F.; Teixeira, F.J.C.S.N.; Zopounidis, C. Artificial intelligence, digital transformation and cybersecurity in the banking sector: A multi-stakeholder cognition-driven framework. *Res. Int. Bus. Financ.* **2022**, *60*, 101616. [CrossRef]
67. Öztürk, R.; Kula, V. A general profile of artificial intelligence adoption in banking sector: A survey of banks in Afyonkarahisar province of Turkey. *J. Corp. Gov. Insur. Risk Manag.* **2021**, *8*, 146–157. [CrossRef]
68. Finkelstein, S.; Hambrick, D.C. Top-Management-Team Tenure and Organizational Outcomes—The Moderating Role of Managerial Discretion. *Adm. Sci. Q.* **1990**, *35*, 484–503. [CrossRef]
69. Mutumba, A.J.M. Understanding The Readiness of Banking Industry Employees to Adopt Artificial Intelligence in Frontier Markets. Master's Thesis, University of Pretoria, Pretoria, South Africa, 2018. Available online: https://www.proquest.com/docview/2901495012?pq-origsite=gscholar&fromopenview=true&sourcetype=Dissertations%20&%20Theses (accessed on 2 September 2024).
70. Maroufkhani, P.; Ismail, W.K.W.; Ghobakhloo, M. Big data analytics adoption model for small and medium enterprises. *J. Sci. Technol. Policy Manag.* **2020**, *11*, 171–201. [CrossRef]
71. Twati, J.M.; Gammack, J.G. The impact of organisational culture innovation on the adoption of IS/IT: The case of Libya. *J. Enterp. Inf. Manag.* **2006**, *19*, 175–191. [CrossRef]
72. Lai, V.S.; Guynes, J.L. An assessment of the influence of organizational characteristics on information technology adoption decision: A discriminative approach. *IEEE Eng. Manag.* **1997**, *44*, 146–157. [CrossRef]
73. De Arroyabe, I.F.; Arranz, C.F.; Arroyabe, M.F.; de Arroyabe, J.C.F. Cybersecurity capabilities and cyber-attacks as drivers of investment in cybersecurity systems: A UK survey for 2018 and 2019. *Comput. Secur.* **2023**, *124*, 102954. [CrossRef]
74. Lekezwa, S.; Zulu, V.M. Critical factors in the innovation adoption of heated tobacco products consumption in an emerging economy. *Int. J. Innov. Sci.* **2023**, *15*, 302–316. [CrossRef]
75. Baldwin, J.; Lin, Z.X. Impediments to advanced technology adoption for Canadian manufacturers. *Res. Policy* **2002**, *31*, 1–18. [CrossRef]
76. Spinellis, D.; Giannikas, V. Organizational adoption of open source software. *J. Syst. Softw.* **2012**, *85*, 666–682. [CrossRef]
77. Abidin, M.A.Z.; Nawawi, A.; Salin, A.S.A.P. Customer data security and theft: A Malaysian organization's experience. *Inf. Comput. Secur.* **2019**, *27*, 81–100. [CrossRef]
78. Chitimira, H.; Ncube, P. The regulation and use of artificial intelligence and 5G technology to combat cybercrime and financial crime in South African Banks. *Potchefstroom Electron. Law J. (PELJ)* **2021**, *24*, 1–33. [CrossRef]
79. Taddeo, M. Three ethical challenges of applications of artificial intelligence in cybersecurity. *MindMach* **2019**, *29*, 187–191. [CrossRef]
80. Yeoh, P. Artificial intelligence: Accelerator or panacea for financial crime? *J. Financ. Crime* **2019**, *26*, 634–646. [CrossRef]
81. Raban, Y.; Hauptman, A. Foresight of cyber security threat drivers and affecting technologies. *Foresight* **2018**, *20*, 353–363. [CrossRef]
82. Thisarani, M.; Fernando, S. Artificial intelligence for futuristic banking. In Proceedings of the 2021 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC), Cardiff, UK, 21–23 June 2021; pp. 1–13. [CrossRef]
83. Payne, E.M.; Peltier, J.W.; Barger, V.A. Mobile banking and AI-enabled mobile banking The differential effects of technological and non-technological factors on digital natives' perceptions and behavior. *J. Res. Interact. Mark.* **2018**, *12*, 328–346. [CrossRef]
84. Lee, J.-C.; Chen, X. Exploring users' adoption intentions in the evolution of artificial intelligence mobile banking applications: The intelligent and anthropomorphic perspectives. *Int. J. Bank Mark.* **2022**, *40*, 631–658. [CrossRef]

85. Ryzhkova, M.; Soboleva, E.; Sazonova, A.; Chikov, M. Consumers' perception of artificial intelligence in banking sector. *Proc. SHS Web Conf.* **2020**, *80*, 01019. [CrossRef]
86. Khan, U.P.; Anwar, M.W. Cybersecurity in Pakistan: Regulations, Gaps and Way Forward. *Cyberpolitik J.* **2020**, *5*, 1–14.
87. Gercke, M. *Understanding Cybercrime: A Guide For Developing Countries*; ITU: Geneva, Switzerland, 2016.
88. Zatarain, J.M.N. The role of automated technology in the creation of copyright works: The challenges of artificial intelligence. *Int. Rev. Law Comput. Technol.* **2017**, *31*, 91–104. [CrossRef]
89. Wang, V.; Nnaji, H.; Jung, J. Internet banking in Nigeria: Cyber security breaches, practices and capability. *Int. J. Law Crime Justice* **2020**, *62*, 100415. [CrossRef]
90. Sarma, M.; Matheus, T.; Senaratne, C. Artificial Intelligence and Cyber Security: A New Pathway for Growth in Emerging Economies via the Knowledge Economy? In *Business Practices, Growth and Economic Policy in Emerging Markets*; World Scientific Publishing: Singapore, 2021; pp. 51–67. [CrossRef]
91. Cavus, N.; Mohammed, Y.B.; Gital, A.Y.; Bulama, M.; Tukur, A.M.; Mohammed, D.; Isah, M.L.; Hassan, A. Emotional Artificial Neural Networks and Gaussian Process-Regression-Based Hybrid Machine-Learning Model for Prediction of Security and Privacy Effects on M-Banking Attractiveness. *Sustainability* **2022**, *14*, 5826. [CrossRef]
92. Donepudi, P.K. Crossing point of artificial intelligence in cybersecurity. *Am. J. Trade Policy* **2015**, *2*, 121–128. [CrossRef]
93. Patil, P. Artificial intelligence in cybersecurity. *Int. J. Res. Comput. Appl. Robot.* **2016**, *4*, 1–5.
94. Mohammed, I.A. Artificial intelligence for cybersecurity: A systematic mapping of literature. *Int. J. Innov. Eng. Res. Technol.* **2020**, *7*, 172–176.
95. Ammirato, S.; Sofo, F.; Felicetti, A.M.; Raso, C. A methodology to support the adoption of IoT innovation and its application to the Italian bank branch security context. *Eur. J. Innov. Manag.* **2018**, *22*, 146–174. [CrossRef]
96. Mallidi, R.K.; Sharma, M.; Singh, J. Legacy Digital Transformation: TCO and ROI Analysis. *Int. J. Electr. Comput. Eng. Syst.* **2021**, *12*, 163–170. [CrossRef]
97. Kumar, A.; Singh, R.K.; Swain, S. Adoption of technology applications in organized retail outlets in India: A TOE model. *Glob. Bus. Rev.* **2022**, 09721509211072382. [CrossRef]
98. Hubbart, J.A. Organizational Change: The Challenge of Change Aversion. *Adm. Sci.* **2023**, *13*, 162. [CrossRef]
99. Malik, S.; Chadhar, M.; Vatanasakdakul, S.; Chetty, M. Factors Affecting the Organizational Adoption of Blockchain Technology: Extending the Technology–Organization–Environment (TOE) Framework in the Australian Context. *Sustainability* **2021**, *13*, 9404. [CrossRef]
100. Tadesse, S. The economic value of regulated disclosure: Evidence from the banking sector. *J. Account. Public Policy* **2006**, *25*, 32–70. [CrossRef]
101. Nayak, R. Banking regulations: Do they matter for performance? *J. Bank. Regul.* **2021**, *22*, 261–274. [CrossRef]
102. Rzepka, C.; Berger, B. User interaction with AI-enabled systems: A systematic review of IS research. In Proceedings of the Thirty Ninth International Conference on Information Systems, San Francisco, CA, USA, 13–16 December 2018.

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.