risks

Review

A Survey on AI Implementation in Finance, (Cyber) Insurance and Financial Controlling

Aleksandrina Aleksandrova *, Valentina Ninova and Zhelyo Zhelev *

Tsenov Academy of Economics, 5250 Svishtov, Bulgaria

* Correspondence: a.alexandrova@uni-svishtov.bg (A.A.); zh.zhelev@uni-svishtov.bg (Z.Z.); Tel.: +359-88-813-8638 (A.A.); +359-88-275-2642 (Z.Z.)

Abstract: Artificial intelligence is changing the world in unprecedented ways and redefining all areas of human activity. In recent decades, the development of AI has progressed at an extraordinary pace. This study examines the scope of implementing AI in the financial sector, insurance, and financial controlling. The research team focuses on these areas, as the main objective of this review is to provide a comprehensive walk-through and to fill the gaps in the literature related to AI implementation in finance, insurance, and financial control from an economic perspective. We provide a comprehensive overview of AI implementation in finance, insurance, and financial controlling, highlighting crucial issues in that process and identifying the relationship between the development of these economic sectors and AI. The authors' team identifies the trends and main themes in the existing literature in AI-related publications in finance, insurance, and financial control. We discuss the main advantages and disadvantages of AI implementation, identified by our research, and also make some suggestions regarding future research having in mind the interdisciplinary of the topic, the vast development of AI and technologies, and the increasing demand for AI-based solutions, services and products.

Keywords: financial products; cyber insurance; financial crimes; bibliometric analysis; systematic review

check for updates

Citation: Aleksandrova, Aleksandrina, Valentina Ninova, and Zhelyo Zhelev. 2023. A Survey on AI Implementation in Finance, (Cyber) Insurance and Financial Controlling. *Risks* 11: 91. https://doi.org/10.3390/risks11050091

Academic Editors: Montserrat Guillén and Mogens Steffensen

Received: 5 February 2023
Revised: 20 April 2023
Accepted: 8 May 2023
Published: 11 May 2023

1. Introduction

In today's world, struggling with a number of multi-layered and complex systems, organizations in the financial sector are striving to improve their digital services to achieve an edge. To achieve this goal, they must adopt agile approaches that prioritise the customer and their dynamically changing needs. This helps organizations improve the bottom line by implementing programs and creating procedures, automating repetitive tasks, and improving customer service (Schroer 2022). Creating open technologies that are always available and easy to use are the new services that attract and retain the customer. Artificial intelligence (AI) is the technology that is coming to the fore. The simulation of embedded human intelligence in machines that are programmed to solve real-world problems is a multifaceted technology aiding the financial sector.

The evolution of AI has weaved multiple sectors, including finance and insurance, towards accelerated development. In terms of finance, artificial intelligence and the digitalization of processes have fundamentally changed not only financial markets but also the attitude of customers of financial institutions, their understanding of financial products and services, etc. To a significant extent, AI-based tools that banks, financial institutions, insurance institutions and non-banks are using such as chatbots, customer service, etc. are accelerating the financial inclusion of individuals. On the other hand, AI-based technologies have revolutionized the financial and insurance market in terms of products and services offered. The development of digital financial services, in particular digital payments (Bansal et al. 2019), led to changes in the ways of committing financial crime (Piper and Metcalfe 2020). As a result, the traditional approaches used by financial control institutions are largely ineffective. They have therefore increased the costs they invest in the fight against financial fraud (LexisNexis 2019). Evolution in the acceleration and promotion of information technology increases financial risk (Du et al. 2022), leading to increased controls to counter financial fraud.

Regarding the terminology, our team adopts the approach of using "artificial intelligence" and not "machine learning" or "data science" because AI is a technology that enables a machine to simulate human behaviour, i.e., to perform actions for decision-making and machine learning is a subset of AI, which allows a machine to automatically, learn from past data without programming explicitly. In modern financial theory, the algorithms of machine learning and in particular support vector machines, falling within the scope of artificial intelligence, find their application for studying banking processes (Zahariev et al. 2022). In the course of conducting the research, we reviewed research articles by authors such as Mirete-Ferrer; Garcia-Garcia; Baixauli-Soler and Prats (Mirete-Ferrer et al. 2022) which address in depth the theoretical background of both machine learning and finance and machine learning methods applied, a discourse different from the one applied in this work, whose research interest is aimed at the implementation of AI in finance, insurance and financial controlling which is predominantly related to performing actions that are in the scope of AI.

This study is part of a larger research project whose main objective is to analyse the effects of AI implementation on the economy. The authors' team's main research fields are finance, insurance, and control. This particular literature review is the starting point for our major research. We focus on the areas mentioned, as our main objective is to provide a comprehensive walk-through and to fill the gaps in the literature related to AI implementation in finance, insurance, and financial control from an economic perspective.

The authors' team decided to conduct a systematic review using the PRISMA method and to perform a thematic analysis of the data obtained.

To accomplish the objective, the authors set out to address the following research questions:

Research Question 1: What are the trends in AI-related publications in finance, insurance, and financial control?

Research Question 2: What are the main themes in the existing literature on finance, insurance, and financial control?

Research Question 3: What are the advantages and disadvantages of implementing AI in the field of finance, insurance, and financial control?

Research Question 4: What are the directions for future research?

The article is organized as follows: Section 2 reviews the literature on AI implementation in finance, insurance, and financial control; Section 3 contains the data used and the methodology performed. Section 4 presents the results of the analysis. Section 5 discusses the results obtained and Section 6 consists of concluding remarks, limitations, and future work.

The main contribution of our research is on the one hand related to the economic view of the problem and on the other hand to the interdisciplinary nature of the topic. The dynamics in the evolution of AI and its symbiosis with the development of services in the financial and insurance sectors, as well as the possibilities for its application in financial control, underline the interdisciplinary nature of the research and create opportunities for expanding the research spectrum in future studies by researchers interested in related research topics.

2. Overview of the Implementation of AI in Finance, (Cyber) Insurance, and Financial Control

Artificial intelligence was first introduced in 1956, but as Fletcher (2018) notes, AI progress is slow. However, AI has been accepted by society, and in the business sphere, it is widely used in all industries and stages of the economy. Moreover, the technologies deployed in AI are crucial to maintain a good position in front of the competition (AL-Rawashdeh and Mamat 2019).

Artificial intelligence is seen as a threat to employment as it is thought to displace the human hand. A similar threat applies to the financial sector, to financial services (Marria 2018). The evolution of AI has created conditions for systems to act and think like humans. Monotonous, often repetitive jobs that basically make logical decisions will be replaced by AI. This will increase work efficiency and save costs in the long run (Manjaly et al. 2021).

In finance, companies that use innovative technology services and products are called FinTech companies. According to (Mhalaga 2020) companies are using AI to encourage people to participate in the financial market. Financial services companies are increasingly embracing digital services due to growing customer demand for digital products and the threat from technology-savvy startups. Some authors (Moro-Visconti et al. 2020) focus their research on the Business Model Scalability and Market Valuation based on the fact that FinTechs and banks operate in the same financial business (although with different features) and share similar clients. FinTech is touted as a game changing, disruptive innovation capable of shaking up traditional financial markets (Lee and Shin 2018). Since it is a frequent practice that banks can internalize a FinTech by buying it and FinTechs and traditional banks share a common market (Agarwal and Zhang 2020), with competition strategies that reduce the conflicts of interest and other governance concerns, the spectrum of AI implementation in finance, financial companies and banking is even more various from one point of view and a gamechanger regarding the future opportunities of uniting businesses and technologies. A step forward this direction are the neobanks and financial technology companies that offers banking services such as Revolut. Along these lines, by the end of 2021, global banks' spending on information technology has risen to USD 297 billion (Rahman et al. 2022).

Outside the technology sector, the financial services sector is a consumer of services provided by AI and is growing rapidly (Cao et al. 2020). Capital markets, trading, banking, insurance, leading/borrowing, investments, asset/wealth management, risk management, marketing, compliance and regulation, payment, contracting, audit, accounting, financial infrastructure, blockchain, financial operations, financial services, financial security (Arner et al. 2015) and financial ethics are covered by finance.

The business environment is also undergoing changes. The introduction of innovations leads to the development of entrepreneurship infrastructure (Raut et al. 2022). The business environment is also undergoing changes. The introduction of innovations leads to the development of entrepreneurship infrastructure. In large part, this is due to the standardization of technologies that can identify and manage. In addition, public resources that contain basic scientific knowledge and funding opportunities are being incorporated into the established infrastructure.

Some authors (Fuji et al. 2020) divide the emergence of artificial intelligence into three waves. The first wave focuses on logical algorithms to carry knowledge. In the second wave, statistical models are implemented to help process data, which we call big data. In the third wave, explanatory models are developed that are capable of applying human qualities such as reasoning to accept tasks and make decisions in certain situations.

The topic of cyber insurance, as part of the approbation of artificial intelligence in practice, has invariably become a key research topic for scholars who apply a different discourse in their research and analysis. Terms encountered in the global literature such as (1) cyber security (cybersecurity, computer security, or information technology security—IT security) (Schatz et al. 2017; Encyclopaedia Britannica 2022); (2) cyber risk (information technology risk, IT risk or IT-related risk) (nibusinessinfo.co.uk n.d.; Joint Technical Committee ISO/IEC JTC1 2013); (3) cyber insurance; and (4) application of artificial intelligence in insurance (Kumar et al. 2019), are not considered abstract concepts, but specialized terminology, progressively entering more and more diverse businesses and industries, a direct projection of the ongoing processes of digitalization of the same. The dynamics of emerging risks follow the development trend of the modern world, in the context of the massive use of digital technologies in combination with artificial intelligence. Threats with cyber genesis, to business and society, require an adequate response, including from the insurance business.

Scientific developments in the insurance field, addressing the topic of cyber insurance, inevitably draw the public's attention to cyber risks. In their work, Carla Barracchini and Via G. Gronchi "Cyber Risk and Insurance Coverage: An Actuarial Multistate Approach" (Barracchini and Addessi 2014), propose the coverage of cyber risks to be implemented in the following way: "On the analogy of the coverage regarding health insurance and following an actuarial multistate approach, three levels of damage will be identified about the functionality of the terminal" (Barracchini and Addessi 2014).

In evidence of the above, authors Kumar, Srivastava, and Bisht defend the idea that "AI can have huge implementation in this sector from predicting risk more accurately than actuary to understanding the new vulnerabilities in the system infrastructure and processes". (Kumar et al. 2019).

The application of artificial intelligence puts the angle of some research papers on the relationship between cyber risk and cyber insurance. In the first of them, Eling and Schnell state that "the immense difficulties to insure cyber risk, especially due to a lack of data and modelling approaches, the risk of change and incalculable accumulation risks" (Eling and Schnell 2016). In 2020, a Special Issue of The Geneva Papers on Risk and Insurance-Issues and Practice on Cyber Insurance was published on cyber risks and cyber insurance (Boyer 2020).

Kesan, Jay P., and Linfeng Zhang propose a method that classifies cyber incidents based on their consequential losses for insurance and risk management purposes (Kesan and Zhang 2020). Applying the method, the relationship between the causes and outcomes of incidents can be further revealed. Kai-Uwe Schanz analyses the current cumulative global cyber incident losses and today's cyber premiums generated by the insurance industry (Schanz 2018).

Another research focus is on measuring market concentration. In the publication "On market concentration and cybersecurity risk", a research team including Dan Geer, Eric Jardine, and Eireann Leverett presents a study on the market concentration of cybersecurity-related risks (Geer et al. 2020). Amanda Hoxell, in her study, Observable Cyber Risk and Market Concentration, also observes the market concentration of cyber risks, outlining the basic pricing principles that are key to any valuation in the context of cyber insurance. She defines the main issues in the cyber insurance market: data quality and availability (Hoxell 2020).

After having presented one part of the research on cyber risks and their relation to cyber insurance, attention will be focused on another group of authors and their research works focused on the cyber security-cyber insurance relation in the process of artificial intelligence application in science and business. In 2018, Levite, Kannry, and Hoffman presented in a publication to the scientific community, their reasoning that harnessing the full potential of cyber insurance "will be imperative not only for managing corporate cyber risks, but for preventing potential systemic cyber incidents of growing concern for governments and the private sector alike" (Levite et al. 2018). In 2020, Dambra, Bilge, and Balzarotti formalized the results of the research conducted, concluding that "SoK: Cyber Insurance - Technical Challenges and a System Security Roadmap" and noted that, "firms are increasingly adopting cyber insurance as part of their corporate risk management strategy" (Dambra et al. 2020).

In his work, "Ransomware Protection Playbook", Roger Grimes notes the following, "Cybersecurity insurance would cover paying the ransom, restoration costs, and business interruption costs-up to the limit of the coverage" (Grimes 2022). In 2022, Puławska, Strzelczyk, and Orzechowski conducted a study and confirmed the sustained and logical increase in interest in cybersecurity insurance (Puławska et al. 2022).

Eling, Martin, and Jingjing Zhu examine the relationship between corporate characteristics and the supply of cyber insurance in the U.S. insurance industry (Eling and Zhu 2018). The results show that insurers with more capital, lower asset risk, greater diversification across business lines and geographies, and group members are more likely to underwrite cyber insurance. In their article (Xie et al. 2020) Xie, X., Lee, C., and Eling, M. examine the determinants of cyber insurance participation, the amount of coverage offered, and the performance of current cyber insurers in the United States. They find that insurers participate in cyber insurance to offset constraints to business growth. In addition, they conclude that the type (stand-alone or bundled) and amount of coverage offered, vary significantly depending on the companies' characteristics (Xie et al. 2020).

3. Data and Methodology

To perform a thematic analysis, we searched the most popular databases Web of Science and Scopus for literature from 2013 to 2023. The team chose these two databases because of their strength and prominence in the emerging technology research field. The following subject areas have been included in the timeline: business, management and accounting; computer science; decision sciences; economics, econometrics and finance; artificial intelligence and machine learning; economics and security systems. The search string, we used in the article was determined by the purpose of the study and the scope of the review, and it includes the following keywords: Artificial Intelligence, Finance, Insurance, Cyber Insurance, Financial controlling applied to the databases was: "artificial AND intelligence AND finance AND controlling"; "artificial AND intelligence AND finance"; artificial AND intelligence AND financial controlling"; "artificial AND intelligence AND insurance". The research team used broad search parameters and generic best-fit phrases to find a variety of sources. Following that, we manually compared, analysed and contrasted search lists. On the next stage of our research, studies that were not aligned with the purpose of the review were eliminated from the search. In this way, items from previous searches were discarded. If the initial search produced no Following that, we discarded items from previous searches. If the initial search delivered no significant results, a narrower syntax would be performed. We obtained the most relevant search by utilizing a specific syntax, and then we narrowed it down to AIs implementation in finance, insurance and financial controlling. Following the research logic, in January 2023, the team selected 4072 relevant articles. Our team chose to implement the PRISMA search strategy, because it is an evidence-based minimum set of items for reporting in systematic reviews and meta-analyses (Moher et al. 2009). PRISMA primarily focuses on the reporting of reviews evaluating the effects of interventions but can also be used as a basis for reporting systematic reviews (PRISMA 2023) and the authors team believes it is an appropriate scientifically proved method which will enhance the quality of this literature review. We excluded from the focus of our study articles that are duplicative, not in English, and those that examine the evolution and implementation of artificial intelligence in finance, insurance, and control from an engineering and information technology perspective. Given the purpose of our study, we selected articles that explore the extent of AI implementation in finance, insurance and control and its effects. We checked the articles mentioned above for duplicates and filtered the results using the inclusion/exclusion criteria that brought to 140 articles assessed for eligibility. As a result of applying the PRISMA search strategy (preferred reporting elements for systematic reviews and meta-analysis), 71 literature sources were selected. The logical structure of the analysis performed is presents in Figure 1 PRISMA diagram detailing the selection process of the academic research articles identified.

We performed a thematic analysis of the seventy-one articles that were selected and qualified for the review. According to Virginia Braun and Victoria Clarke, thematic analysis is a method for analysing qualitative data that entails searching across a data set to identify, analyse, and report repeated patterns (Braun and Clarke 2006). Applying this method, the research team grouped the articles based on their theme similarity. Following the thematic analysis algorithm, we determined each article's relevance to one of the core topics by reviewing the abstract and the content of the papers. As a result of the qualitative analysis of the articles, 12 themes and subthemes were identified. These themes include artificial intelligence, financial management, banking, technology, chatbot assistance, customer and consumer decision-making, financial inclusion, machine learning, insurance, cyber insurance, fraud detection, financial controlling, and cybersecurity. Comprehensive themes such as "Finance", "Insurance", and "Financial controlling" are included alongside more specific sub-themes. Some of these research topics refer to relatively fewer research results, which may lead to identifying possible research gaps.

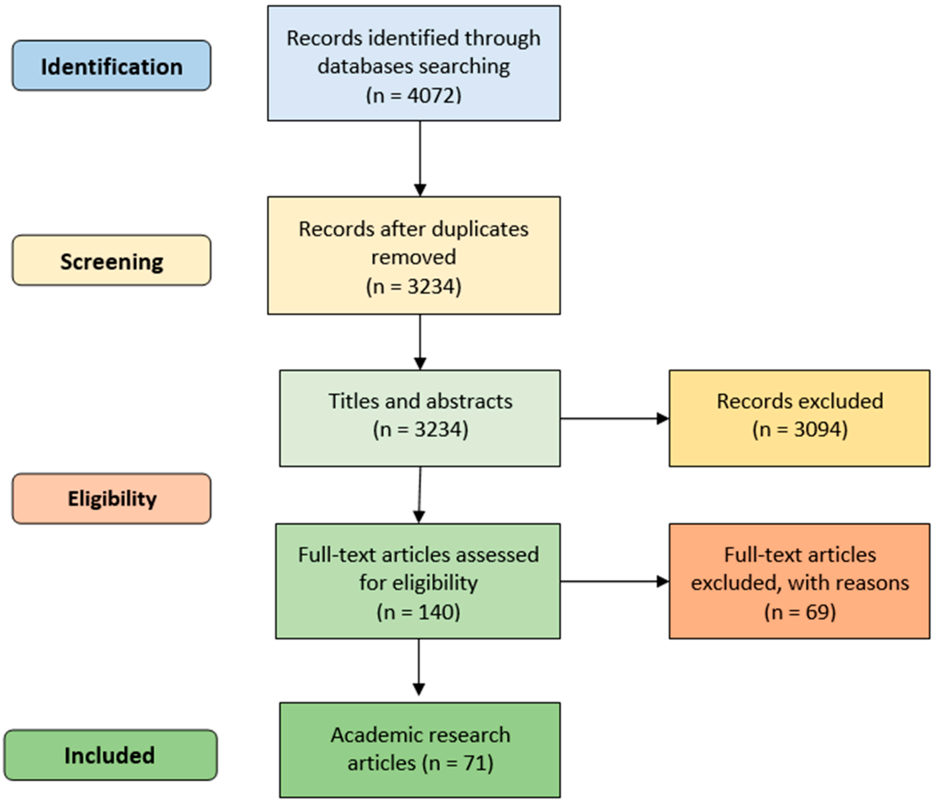
Identification
Records identified through databases searching (n = 4072)
Screening
Records after duplicates removed (n = 3234)
Titles and abstracts (n = 3234)
Records excluded (n = 3094)
Eligibility
Full-text articles assessed for eligibility (n = 140)
Full-text articles excluded, with reasons (n = 69)
Included
Academic research articles (n = 71)

Figure 1. PRISMA diagram detailing the selection process of the academic research articles identified. Source: (Moher et al. 2009), authors' interpretation.

4. Results

4.1. Implementation of AI in Finance

The social demand for and expectations from artificial intelligence in the financial sector are high. Given this perspective, the amount of investment in this field is larger compared to other industries such as the distribution, manufacturing, and public sectors (Okuda and Shoda 2018). From one point of view, AI in finance refers to the applications of AI techniques in financial businesses (Longbing 2022) and from the other, the researchers focus on the role of AI, which is transforming financial world and fostering financial inclusion through the widespread use of algorithms to automate risk detection management and measurement (Peric 2015); (Muneeza et al. 2018). Many recent studies examine the combination of AI and the financial sector because anyone who engages in economic activities is a financial consumer. Furthermore, even software used exclusively by traditional asset managers can be downloaded easily and used by ordinary people (Malali and Gopalakrishnan 2020). AI has a strong influence on digital financial inclusion in areas related to risk detection, measurement and management, addressing the problem of information asymmetry, availing customer support and helpdesk through chatbots and fraud detection and cybersecurity (Mhalaga 2020).

In the context of the application of AI in finance, researchers are examining the synergy between the AI based features and FinTech. Artificial intelligence (AI) with its highly cognitive features has been increasingly adopted by FinTech firms. With increasing market and economic fluctuations during the unprecedented times of COVID-19, AI offers high computational and easily accessible personalized financial solutions (Yadav et al. 2022). FinTech today includes some of the significant areas such as bitcoin and blockchain technology and a novelty in the financial market that are so-called "neobanks", banks without physical locations (Martincevic et al. 2022). This makes the use of artificial intelligence in these financial spheres increasingly common.

Considering banking as one of the fundamental implications of finance, the vast development and implementation of bank products, and the demand for delivering new attractive features to bank consumers, AI has a broad implication in many banking activities. Banks and non-banking institutions are building on digital ways that were in use for years through the direct application of artificial intelligence (AI) to improve access even to the people who were previously served by the formal financial institutions (Alameda 2020; Peric 2015). Through the use of AI, banks are now adopting customer support and help desks which are impacting more on increasing efficiency and reducing the cost of customer support (Mhalaga 2020). With AI, financial institutions can provide personalized banking where chatbots and AI assistants (Hwang and Kim 2021), use AI to come up with personalized financial advice and natural language processing to provide instant, self-help customer service (Alameda 2020; Peric 2015). A chatbot is a communication software that can store appropriate answers to questions on a server, create models that continuously develop correct answers through conversations with customers, control exceptions, and provide accurate answers (Serban et al. 2017). Chatbots create a self-learning model through computer programs and mathematical calculations and provide customers with answers and other relevant information as close as possible to user questions in real time. For companies, a chatbot is an interface that provides information required by customers and marketing through communication with financial consumers (Yu et al. 2020).

The rapid development of Internet fostered the evolution of artificial intelligence and the demand of AI based solutions in banking. The vigorous development of AI has provided a good opportunity for mobile payment (Xu and Song 2021). Mobile payment is the process that consumers use mobile phones, bracelets, and other electronic devices in their daily life to complete payment of the commodity (Nelloh et al. 2019). Mobile payment is a brand-new payment method formed by the combination of four channels: Internet, mobile client, terminal equipment, and financial institutions (Liao 2020) The era of AI has brought infinite vitality to the development of MP, which in turn enriches the types of AI technology (Tsai et al. 2017). With the advent of AI, the application scenarios of mobile payments are constantly expanding (Hsiao 2020).

Some of the research papers analysed examine AI implementation not in financial products and services but in financial management. After a lot of investigation and practice by scientific researchers, the modern financial management system is different from the previous accounting-based accounting management system and expands other business operations on the basis of the traditional financial management system (Chornovol et al. 2020). To better promote the healthy and long-term development of corporate financial management, the basement is established on the perspective of artificial intelligence (AI) (Xu and Song 2021). Certainly, AI/ML has found practical applications in finance; whether it is generating insights on customer spending, obtaining informed underwriting risk outcomes, detecting anomalous fiscal transactions or interacting with customers using natural language, AI/ML potentials in finance is gaining significant momentum in today's world of near ubiquity Internet of Things (IoT), advanced computing and telecommunication technologies (Eluwole and Akande 2022). Financial budget management system mainly has functions such as budget preparation, budget adjustment, budget control, and budget analysis (Qin and Qin 2021). The preparation of a comprehensive budget is the starting point for business management and control of daily economic activities.

4.2. AI Implementation in Cyber Insurance and Cyber Security

The topic of cyber security, in the context of the application of artificial intelligence, is increasingly on the agenda of science, society, business, and politics because cyber-attacks continue to grow in number and intensity, and cyber threats are increasingly diverse in nature, making them extremely relevant. The emerging negative trend towards increasing cyber security threats predetermines the increased demand for, and supply of, protection aimed at neutralizing and minimizing the damage caused by the manifestation of cyber risks.

The European Union has established and operates a dedicated structure dedicated to achieving a high common level of cyber security—the European Union Agency for Cybersecurity (ENISA) (European Union Agency for Cybersecurity (ENISA) (2022)). In 2020, ENISA published a report aimed at building a National Capabilities Assessment Framework (NCAF), which aims "at providing Member States with a self-assessment of their level of maturity by assessing their NCSS objectives, that will help them enhance and build cybersecurity capabilities both at strategic and at the operational level."(European Union Agency for Cybersecurity (European Union Agency for Cybersecurity (ENISA) (2020)). In 2022, Munich Re released the results of a report compiled following a global survey on cyber risk and insurance (involving more than 7000 participants from 14 countries, all industries, and company sizes). The results it presents are more than alarming, with 83% of those who participated in the survey stating that the level of cybersecurity is not sufficiently guaranteed (Munich Re 2022). A study by Cybersecurity Ventures predicts that losses due to the realization of IT risks will amount to approximately USD 10.5 trillion in 2025 (Cybersecurity Ventures 2020) (Munich Re). Allianz Global Corporate and Specialty's ranking of the most significant business risks for 2022 is topped by cyber incidents (Allianz Global Corporate and Specialty 2022), and according to Lloyd's. Swiss Re, the global cyber insurance market is expected to grow rapidly to USD 18 billion by 2025 (Schanz 2018). The results of the cited studies can be taken as a valid reason for a paradigm shift: from considering insurance protection as a solid cost for the government and businesses to perceiving it as an investment with high returns. In this regard, insurance is a kind of instrument that guarantees both the prevention and repression of cyber risks.

4.3. Artificial Intelligence and Financial Control in the Fight against Financial Crime

Artificial intelligence is also implemented in public finance and the regulation of government-business relations. The application of artificial intelligence in financial relations between public authorities and businesses is increasingly common, especially in financial control. Financial control bodies monitor the legality of expenditure and revenue orders. The aim is to limit the damage that can be caused by the commission of illegal acts by economic operators. Financial control is a specialised control which includes checks and analyses (Kulchev 2021) of the economic and financial activity, to establish the legality of the materials and financial means used. Financial control can also be defined as a specific instrument to prevent illegal financial actions by applying documentary control on the financial records of economic entities (Beldiman 2022).

Control institutions use artificial intelligence to detect financial crime (FSB 2017). In machine learning, algorithms are specified that can be used to identify suspicious transactions, assess their risk, and track them in detail and/or preventively limit them (Deloitte 2018). For example, the Australian Securities and Investments Commission (ASIC) uses natural language technology capabilities to extract evidential information (FSB 2017). Because suspicious transactions take a long time to investigate, those transactions that pose a higher risk are identified (Prove 2021).

Artificial intelligence is applicable in the work of control authorities when they apply risk assessment (Kostova 2013). In this method, a created data repository is used to capture risky economic entities that fall within the hypotheses of predefined criteria. In this way, models are created involving planning, searching, inference and even interpolation of results at a high level. Moreover, human subjectivity is limited to minimal values.

More and more people around the world are falling victim to attacks on their privacy and information. There has been a significant growth in cybercrime. One of the reasons is the rapid adaptation of cyber criminals to new technologies. Additionally, the increase in consumers shopping online. Another reason that can be attributed is countries that do not allocate sufficient financial resources for protection, respectively, are frequently attacked through cyber-attacks. These are mainly poorer countries with low incomes and weak economies. In a report, the Centre for Strategic and International Studies (CSIS), in partnership with the cybersecurity company—McAfee (Lewis 2018) point out that countries such as Russia, North Korea, and Iran are the most active in hacking financial institutions (Lewis 2018).

Artificial intelligence has not yet reached the level necessary for total countermeasures. AI is expected to play an important role in the future fight against financial crime. At this point in time, AI used for financial fraud is seen as an accompanying factor, as a tool to carry out the act (King et al. 2020). There are certain limitations in the use of AI for investigating financial crimes and rather for seeking criminal liability. These are twofold, firstly, whether AI will be able to answer the question relating to the subjective element of guilt (criminal intent) and secondly, the assessment of whether there has been a constitutive criminal act (Macdonald 2015).

5. Discussion

Artificial intelligence is widely implemented in the finance. In the banking sector, it is applied in two aspects—on the one hand, for process administration and information management in bank institutions, and on the other hand for improving customer service, increasing customer satisfaction, financial inclusion, etc. Artificial intelligence is also widely applied in financial management, financial analysis and many operations related to financial governance. Undoubtedly, AI is an accelerator for the development of these sectors, as its increasing application implies an ever-wider range of new products and services that make the companies that exploit it increasingly competitive. Digitalisation in every aspect of social and economic life is also a factor in the development of AI-based technologies and solutions in finance. Consumers are looking for more digital tools and solutions that companies and banks need to provide them. In turn, the availability of such products and services is accelerating financial inclusion.

As the application of artificial intelligence increases in many areas related to service delivery, controversial issues regarding ethical considerations in the use of AI are growing. As the discipline of AI grows, it begins to expand into fields of decision-making, such as credit rating and banking, and can have significant impact on people's lives. The ethical and moral issues associated with AI are important issues which need to be further explored in studies by researchers with expertise in myriad disciplinary and professional domains (How et al. 2020). These ethical and moral issues inevitably raise the problem of replacing the human factor in more and more services and functions, which suggests the loss of jobs. According to a McKinsey & Company's report from 2017, depending upon various adoption scenarios, automation will displace between 400 and 800 million jobs by 2030, requiring as many as 375 million people to switch job categories entirely. In that manner, we should mention that technological change may eliminate specific jobs, but it also creates new ones in the process.

In the research field of insurance, topics concerning the issues of AI, cyber security, cyber risks, and cyber insurance are gaining more and more popularity and are the subject of several research papers—in the discourse of which various issues fall and multifaceted analyses are presented. In one part of the scientific publications, the focus is on the interrelations (between cyber risk and cyber insurance, and between cyber security and cyber insurance), in others, the cyber insurance market is analysed (global, national, and regional), and in others, the market concentration is measured using the commonly accepted toolbox of indices. Despite the wide range of research papers addressing the topic of cyber insurance, the rapid pace of AI development, as well as the threats facing humanity, predetermine the need to present current research on the topic.

Artificial intelligence is used in financial control by control institutions. Due to the huge volume of information, AI assists the process of data identification, analysis and selection. In theory and practice, these actions are known as risk analysis. These are practices that are applied to analyse the probability of occurrence of certain risks. In this way, financial control institutions seek to preventively limit the behaviour of controlled entities that negatively impacts the economic environment. However, financial controls are based on universal and basic theoretical propositions. In order for the AI used in financial control to be effective, far more structured and advanced technologies need to be applied. Their evolution must be at a pace parallel to that at which the negative behaviour of the controlled entities evolves. In the following lines, we will try to identify concrete steps in this direction that would allow AI applied in financial control to be more effective.

The first step is to move from direct influence on risk to indirect influence. At the moment, in the vast majority of cases, the control authorities intervene in deciding which entities should be audited in which areas. AI will be useful if this task is taken on by risk assessors. Their work would thus take a more central role. The second step is directed from dealing with both difficult and easy tasks to more difficult tasks. In a large number of cases, control bodies combine difficult and easy tasks. Thus, a more difficult task may be followed by a small number of easy tasks. In risk-focused work, there will be more concentration on the difficult tasks to be performed. The third step is from working with a large volume of documentation to a timely control impact system. Cluttered filing cabinets, crammed with work in progress and with unpleasant tasks always left in the pile of paperwork is a picture everyone is familiar with. New tools in risk-focused work suggest creating a system for communicating new risks "just in time".

These three pressing changes are a non-exhaustive summary that aims to provide a different perspective on the issues surrounding the use of artificial intelligence in financial controls. Knowledge of such guidance by control authorities and control managers is critical to the successful implementation of risk analysis.

6. Conclusions

With the evolution of artificial intelligence, its application in modern economics is inevitable. Application of AI in all financial, insurance and controlling processes will continue to expand with expanding the possibilities that AI offers to business, government bodies and people to facilitate and administrate better their activities.

Given the research and in-depth study of the literature sources covered in this literature review, we were able to identify the main research topics and directions related to the application of AI in finance, insurance and control. The sources studied allowed us to identify some gaps regarding the literature in these areas, enabling us to direct our future research towards addressing these research gaps. Actually, the identification of these gaps and setting the directions for future research addressing them makes this research paper relevant to the ongoing literature in the thematic areas analysed.

A significant number of the papers analysed, explore the relationship between AI and financial inclusion, with most researchers in the field considering AI to be among the leading factors in promoting and fostering financial inclusion for individuals. The rapid development of FinTech companies and their products, and the close connection of the sector with the development of digital technologies, implies the increasing implementation of AI in this financial sphere.

It can be summarized from the reviewed articles investigating the implementation of AI in the banking sector that researchers focus their research on digital solutions related to customer service and digital banking. Both are significantly related to the development of AI and the spectrum of its application in banking products and services will undoubtedly grow as this market expands. Another aspect is mobile payments, which are constantly expanding with the development of AI.

The continuous transformation of financial products and services contributes to convenient and diversified consumer choice. On the one hand, AI will facilitate complex and multi-component computing, easy and fast transfer of big data, etc. On the other hand, each country and their authorities and institutions will need to introduce and implement new policies to ensure the data protection and financial integrity of their population and business entities. Fast and effective solutions in organizing AI would be a good answer in protecting government and business systems from cyber-attacks (Yeoh 2019). In response to research question 1 and considering the research performed, the authors' team identified the following trends in AI-related publications in finance, insurance, and financial control: research on the correlation between the dynamic development of AI-based applications and technologies and their widespread application in the three mentioned areas; a significant number of papers focus on the opportunities that AI provides for risk identification, process optimization, and development opportunities, emphasizing its role as an accelerator for development. Most of the research in the three areas mentioned focuses on the role of AI as a game-changer and a factor that fosters change in a manner of digitalization, introducing new products and services, improving quality of control processes, etc. On the other hand, much of the literature reviewed lacks specific research on the implementation of AI in the work of control institutions.

Answering research question 2, the main themes we have identified regarding artificial intelligence implementation in finance are focused on AI-based solutions and applications that promote financial inclusion, expand banking services in customer support and e-banking, mobile payments, FinTech products and financial management.

Research developments in insurance related to the topic of cyber insurance inevitably draw public attention to cyber risks. Another body of scholarly work focuses on the relationship between cyber risk and cyber insurance, and a third focuses on the measurement of market concentration. Research papers devoted to cyber insurance also focus on the cybersecurity-cyber insurance nexus in the process of applying artificial intelligence in science and business and explore the relationship between corporate characteristics and the supply of cyber insurance in the insurance industry.

Financial control research focuses on the behaviour of controlled entities. In addition, individual publications focus on the factors determining the development of financial control through the implementation of new technologies. Special attention is paid to the preventive form of control - risk analysis. This is an activity through which control bodies support their activities and pre-select the objects subject to financial control. Although, there is a lack of research on the impact (positive or negative) on the performance of control bodies impacting financial stability. Exploring the level of AI implementation and what challenges control bodies face are topics that will be addressed in the future.

The second group of research papers focuses on the fight against financial crime. Different authors consider the options through which the implementation of AI in financial control allows to limit the possibilities of misconduct on the part of control persons.

Regarding the advantages and disadvantages of AI implementation, an attempt has been made in the Results section and its subsections to indicate what the advantages of AI are in the three areas considered and where it lags or there is a negative sign of usefulness. The research articles reviewed in this study identify the advantages of applying AI in finance, insurance, and financial control primarily through its role as an accelerator for the development of processes and services. This is broadly explained by the nature of AI and its rapid evolution in recent years, which implies its implementation in wider range of fields and activities. The evolution of AI is leading to new areas of application, and digitalization in every aspect of social and economic development is encouraging the search for AI-based solutions in more and more aspects of finance, insurance and control. It is concluded that in the third area, financial control, AI assists control authorities in processing and selecting information, and also analysis in searching for a high probability (risks) of financial fraud. However, shortcomings are still found as the pace of AI development in the public sector is much slower than in the private sector. Regarding finance and insurance, the AI implementation not only forces the development and introduction of new products and services such as new investment instruments, banking services, etc. but also affects financial inclusion through the products used for customer support such as chatbots, etc. On the other hand, AI fostered the introduction of completely new financial markets institutions such as neobanks which imply the characteristics of banks and FinTech companies. The main disadvantages we identified are related to the moral and ethical issues that the application of AI introduces, as well as the discussion raised by some authors regarding the alleged loss of jobs.

Limitations and Future Work

This review is by no means exhaustive and conclusive. According to the research team some limitations exist in the review. The literature review focuses mainly on the implementation of AI in finance, insurance and controlling from the economic point of view and does not consider the evolution in the development of AI from the perspective of its development and improvement. The author's team limits the research to this area as it is part of a larger research project that aims to investigate the effects of AI implementation in economics.

Although we consider practitioners as a relevant expert group, especially, since banks, controlling government bodies and insurance companies have the most comprehensive data on AI implementation and its' effects we did not pinpoint enough relevant industry expertise in this article. Given this, the conclusions in this paper are based on a limited number of academic research articles, and the research itself has the characteristics of a theoretical desk study.

Finally, the review discusses key common features of the implementation of AI in finance, insurance and control globally. Given the extremely rapid development of services in the financial and insurance markets and the increasing symbiosis in their development with that of artificial intelligence, the author's team cannot explore all aspects theoretically and empirically. There are many controversies in the scientific literature often due to the interdisciplinary of the chosen topic, the ethical issues that the development of AI raises, etc. Our study is limited by the systematic framework, which is partly due to these controversies.

Due to the interdisciplinary nature of the topic, we cannot cover all thematic areas, nor can we predict what thematic areas may be covered in the next few years, but we believe our study is valuable in that it could serve as a starting point for researchers interested in related research topics. In response to research question 4, the author team will continue working in the research area as this literature review will be a stepping stone for our future work. Our concrete proposals for the future practical applicability of this research and our team's future work are being addressed within this section. As most of the reviewed articles focus on AI implementation and service development in the financial sector, from a financial perspective, the focus of future research will be financial inclusion and its dependence on AI-based services, as this will also allow us to measure the impact of this implementation. Another topic the authors intend to investigate is the relationship between AI implementation in banking and FinTech, having in mind that both share a common market and similar clients and the rapid development of neobanks. Virtual banks (neobanks) are insufficiently investigated, especially in the manner of implementation of AI and its accelerating effect on their evolution having in mind that they combine technology, customer support, chatbots, new financial and investment products, etc. In other words, neobanks are specifically interesting topic for future research having in mind they incorporate most of the AI implementation aspects in finance reviewed. To compensate for the established vacuum related to the current topics of artificial intelligence, cyber risks, and cyber security in the field of insurance, it is planned to focus future research on the analysis of insurance products offered to address cyber risks and to highlight their specificities in the context of an insurance market. The authors also consider one type of control, financial control, and not control at all. On this basis, the authors focus on financial control and the implementation of AI in managing risks that give rise to the need for financial control. In this way, we believe that future research will be able to assess the extent of the applicability of AI in the area of financial control.

Author Contributions: Conceptualization, A.A., Z.Z. and V.N.; writing—original draft preparation, A.A., Z.Z. and V.N.; project administration, A.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by The Bulgarian National Science Fund at the Bulgarian Ministry of Education and Science, Funding Competition for financial support for projects of junior researchers and postdocs—2022, Funding number: KII-06-M65/2 from 12 December 2022, Project title: "Artificial intelligence in the economic perspective", Project coordinator: Aleksandrina Aleksandrova, PhD.

Data Availability Statement: Upon request from the corresponding author.

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

References

Agarwal, Sumit, and Jian Zhang. 2020. FinTech, lending and payment innovation: A review. *Asia-Pacific Journal of Financial Studies* 49: 353–67. [CrossRef]

Alameda, Teresa. 2020. Data, AI and Financial Inclusion: The Future of Global Banking—Responsible Finance Forum. Available online: https://responsiblefinanceforum.org/data-ai-financial-inclusion-future-global-banking (accessed on 10 March 2023).

Allianz Global Corporate and Specialty. 2022. *Allianz Global Corporate & Specialty. Business Insurer. News & Insights. Reports. Allianz Risk Barometer 2022*. April 22. Available online: https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html (accessed on 10 March 2023).

AL-Rawashdeh, Ghada Hammad, and Rabiei Bin Mamat. 2019. Comparison of four email classification algorithms using WEKA. *International Journal of Computer Science and Information Security (IJCSIS)* 17: 42–54.

Arner, Douglas. W., Janos Nathan Barberis, and Ross P. Buckley. 2015. The Evolution of Fintech: A New Post-Crisis Paradigm? *UNSW Law Research* 47: 1271. [CrossRef]

Bansal, Sukriti, Phill Bruno, Olivier Denecker, and Marc Niederkorn. 2019. *Global Payments Report 2019: Amid Sustained Growth, Accelerating Challenges Demand Bold Actions*. McKinsey Global Payment USA Reports. September 2019, Copyright © McKinsey & Company. Available online: https://www.mckinsey.com (accessed on 10 March 2023).

Barracchini, Carla, and M. Elena Addessi. 2014. Cyber risk and insurance coverage: An actuarial multistate approach. *Review of Economics Finance* 4: 57–69. Available online: http://www.bapress.ca/ref/v4-1/1923-7529-2014-04-57-13.pdf (accessed on 10 March 2023).

Beldiman, Camelia Madalina. 2022. Efficiency and Advantages of Preventive Financial Control versus Internal Control in a Public Entity. *Jurnalul De Studii Juridice* 17: 134–47. [CrossRef]

Boyer, M. Martin. 2020. Cyber insurance demand, supply, contracts and cases. *The Geneva Papers on Risk and Insurance—Issues and Practice volume* 45: 559–63. Available online: https://link.springer.com/article/10.1057/s41288-020-00188-1 (accessed on 10 March 2023). [CrossRef]

Braun, Virginia, and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology* 3: 77–101. [CrossRef]

Cao, Longbing, Qiang Yang, and Philip S. Yu. 2020. Data science and AI in FinTech: An overview. *General Finance* 12: 81–99. [CrossRef]

Chornovol, Alla, Julia Tabenska, Tetiana Tomniuk, and Liudmyla Prostebi. 2020. Public finance management system in modern conditions. *Investment Management and Financial Innovations* 17: 402–10. [CrossRef]

Cybersecurity Ventures. 2020. *Special Report: Cyberwarfare in the C-Suite*. Edited by Steve Morgan. Available online: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/ (accessed on 10 March 2023).

Dambra, Savino, Leyla Bilge, and Davide Balzarotti. 2020. SoK: Cyber insurance–technical challenges and a system security roadmap. Presented at 2020 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, May 18–21; pp. 1367–83. [CrossRef]

Deloitte. 2018. The Case for Artificial Intelligence in Combating Money Laundering and Terrorist Financing: A Deep Dive into the Application of Machine Learning Technology. Available online: https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/finance/sea-fas-deloitte-uob-whitepaper-digital.pdf (accessed on 6 January 2023).

Du, Meijie, Baifang Liu, and Haoyun Zhou. 2022. Construction of financial early warning model based on machine learning technology. Paper presented at International Conference on Multi-Modal, Huhehaote, China, April 22–23; pp. 75–83.

Eling, Martin, and Jingjing Zhu. 2018. Which Insurers Write Cyber Insurance? Evidence from the U.S. Property and Casualty Insurance Industry. *Journal of Insurance Issues* 41: 22–56. Available online: http://www.jstor.org/stable/26441191 (accessed on 10 March 2023).

Eling, Martin, and Werner Schnell. 2016. What do we know about cyber risk and cyber risk insurance? *The Journal of Risk Finance*. Available online: https://www.emerald.com/insight/content/doi/10.1108/JRF-09-2016-0122/full/html (accessed on 10 March 2023).

Eluwole, Opeoluwa Tosin, and Segun Akande. 2022. Artificial Intelligence in Finance: Possibilities and Threats. Presented at 2022 IEEE International Conference on Industry 4.0, Artificial Intelligence, and Communications Technology (IAICT), Bali, Indonesia, July 28–30; pp. 268–73. [CrossRef]

Encyclopaedia Britannica. 2022. Editors of Encyclopaedia. Computer Security. November 18. Available online: https://www.britannica.com/technology/computer-security (accessed on 10 March 2023).

European Union Agency for Cybersecurity (ENISA). 2020. *Publications/Report-Files/Ncaf-Translations/National-Capabilities-Assessment-Framework*. Athens: European Union Agency for Cybersecurity (ENISA).

European Union Agency for Cybersecurity (ENISA). 2022. *Home. News. Is the EU Healthcare Sector Cyber Healthy? The Conclusions of Cyber Europe 2022*. Athens: European Union Agency for Cybersecurity. Available online: https://www.enisa.europa.eu/news/is-the-eu-healthcare-sector-cyber-healthy-the-conclusions-of-cyber-europe-2022 (accessed on 10 March 2023).

Fletcher, John. 2018. Deepfakes, artificial intelligence, and some kind of dystopia: The new faces of online post-fact performance. *Theatre Journal* 70: 455–71. [CrossRef]

FSB. 2017. Artificial Intelligence and Machine Learning in Financial Services. Available online: https://www.fsb.org/wp-content/uploads/P011117.pdf (accessed on 10 March 2023).

Fuji, Masaru, Nakazawa Katsuhido, and Hiroaki Yoshida. 2020. "Trustworthy and Explainable AI" Achieved Through Knowledge Graphsand Social Implementation. *Fujitsu Scientific & Technical Journal* 56: 39–45.

Geer, Dan, Eric Jardine, and Eireann Leverett. 2020. On market concentration and cybersecurity risk. *Journal of Cyber Policy* 5: 9–29. [CrossRef]

Grimes, Roger A. 2022. Cybersecurity Insurance. In *Ransomware Protection Playbook*. Hoboken: Wiley Data and Cybersecurity, pp. 85–112.

How, Meng-Leong, Sin-Mei Cheah, Aik Cheow Khor, and Yong Jiet Chan. 2020. Artificial Intelligence-Enhanced Predictive Insights for Advancing Financial Inclusion: A Human-Centric AI-Thinking Approach. *Big Data and Cognitive Computing* 4: 8. [CrossRef]

Hoxell, Amanda. 2020. Observable Cyber Risk and Market Concentration. Examination Paper in Mathematics, 30 hp. Handledare: Ulrik Franke, RISE Ämnesgranskare: Erik Ekstrom Examiner: Julian Külshammer, October 2020. Available online: https://www.diva-portal.org/smash/get/diva2:1477820/FULLTEXT01.pdf (accessed on 10 March 2023).

Hsiao, Ming-Hsiung. 2020. Mobile payment services as a facilitator of value co-creation: A conceptual framework. *Journal of High Technology Management Research, Science Observation* 15: 79–80. [CrossRef]

Hwang, Sewong S., and Jonghyuk Kim. 2021. Toward a Chatbot for Financial Sustainability. *Sustainability* 13: 3173. [CrossRef]

Joint Technical Committee ISO/IEC JTC1. 2013. *Subcommittee SC 27*. Available online: https://www.iso.org/standard/54534.html (accessed on 10 March 2023).

Kesan, Jay P., and Linfeng Zhang. 2020. Analysis of cyber incident categories based on losses. *ACM Transactions on Management Information Systems (TMIS)* 11: 1–28. [CrossRef]

King, Thomas C., Nikita Aggarwal, Mariarosaria Taddeo, and Luciano Floridi. 2020. Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions. *Science and Engineering Ethics* 26: 89–120. [CrossRef]

Kostova, Silviya. 2013. Audit Procedures for Disclosure of Errors and Fraud In Financial Statements of Bulgarian Companies. *Scientific Annalsof the "Alexandru Ioan Cuza" University of IaşiEconomic Sciences* 59: 49–66. [CrossRef]

Kulchev, Krasimir. 2021. Tools of Economic Analysis When Researching the Tourism Market. *Business Management* 2: 21–37.

Kumar, Naman, Jayant Dev Srivastava, and Harshit Bisht. 2019. Artificial intelligence in insurance sector. *Journal of the Gujarat Research Society* 21: 79–91.

Lee, In, and Yong Jae Shin. 2018. Fintech: Ecosystem, business models, investment decisions, and challenges. *Business Horizons* 61: 35–46. [CrossRef]

Levite, Ariel E., Scott Kannry, and W. Wyatt Hoffman. 2018. *Addressing the Private Sector Cybersecurity Predicament: The Indispensable Role of Insurance*. Washington, DC: Carnegie Endowment for International Peace.

Lewis, James. 2018. Economic Impact of Cybercrime—No Slowing Down. Available online: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf (accessed on 7 January 2023).

LexisNexis. 2019. *LexisNexis Risk Solutions*. Retrieved 2023. Available online: https://risk.lexisnexis.com/insights-resources/research/us-ca-true-cost-of-fraud-study (accessed on 10 March 2023).

Liao, L. 2020. Mobile payment and online to offline retail business models. *Journal of Retailing and Consumer Services Popular Science and Technology* 22: 6–8. [CrossRef]

Longbing, Cao. 2022. AI in Finance: Challenges, Techniques, and Opportunitie. *ACM Computing Surveys* 55: 38. [CrossRef]

Macdonald, S. 2015. *Text, Cases and Materials on Criminal Law*. Harlow: Pearson Education Limited.

Malali, Anil B., and S. Gopalakrishnan. 2020. Application of Artificial Intelligence and Its Powered Technologies in the Indian Banking and Financial Industry: An Overview. *IOSR Journal of Humanities And Social Science* 25: 55–60.

Manjaly, Joel, Ranjana Mary Varghese, and Philip Varughese. 2021. Artificial Intelligence in the Banking Sector—A Critical Analysis. *Shanlax International Journal of Management* 8: 210–16. [CrossRef]

Marria, Vishal. 2018. Is Artificial Intellegence Replacing Jobs in Banking? Available online: https://www.forbes.com/sites/vishalmarria/2018/09/26/is-artificial-intelligence-replacing-jobs-in-banking/?sh=625de1253c55 (accessed on 6 January 2023).

Martincevic, Ivana, Sandra Crnjevic, and Igor Klopotan. 2022. Novelties and benefits of fintech in the financial industry. *International Journal of E-Services and Mobile Applications*. [CrossRef]

Mhalaga, David. 2020. Industry 4.0 in finance: The impact of artificial intelligence (ai) on digital financial inclusion. *International Journal of Financial Studies* 8: 45.

Mirete-Ferrer, Pedro M., Alberto Garcia-Garcia, Juan Baixauli-Soler, and Maria A. Prats. 2022. Review on Machine Learning for Asset Management. *Risks* 10: 84. [CrossRef]

Moher, David, Alessandro Liberati, Jennifer Tetzlaff, and Douglas G. Altman. 2009. The PRISMA Group (2009). Pre-ferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement. *PLoS Medicine* 6: e1000097. [CrossRef]

Moro-Visconti, Roberto, Salvador Cruz Rambaud, and Joaquín López Pascual. 2020. Sustainability in FinTechs: An Explanation through Business Model Scalability and Market Valuation. *Sustainability* 12: 10316. [CrossRef]

Muneeza, Aishath, Asma Tajul Arifin ′, and Nur Aishah Arshad. 2018. The Application of Blockchain Technology in Crowdfunding: Towards Financial Inclusion via Technology. *International Journal of Management and Applied Research* 5: 82–98. [CrossRef]

Munich Re. 2022. Munich Re Global Cyber Risk and Insurance Survey 2022. Available online: https://www.munichre.com/landingpage/en/global-cyber-risk-and-insurance-survey-2022.html#download (accessed on 10 March 2023).

Nelloh, Liza Agustina Maureen, Adhi Setyo Santoso, and Mulyadi Wiguna Slamet. 2019. Will users keep using mobile payment? it depends on trust and cognitive perspectives. *Procedia Computer Science* 161: 1156–64. [CrossRef]

nibusinessinfo.co.uk. n.d. *Home. Guides. IT. IT Security and Risks. IT Risk Management. What Is IT Risk?* Available online: https://www.nibusinessinfo.co.uk/content/what-it-risk (accessed on 10 March 2023).

Okuda, Takuma, and Sanae Shoda. 2018. AI-based chatbot service for financial industry. *Fujitsu Scientific and Technical Journal* 54: 4–8. Available online: https://www.fujitsu.com/global/documents/about/resources/publications/fstj/archives/vol54-2/paper01.pdf (accessed on 10 March 2023).

Peric, Kosta. 2015. Digital financial inclusion. *Journal of Payments Strategy & Systems* 9: 212–14. Available online: https://www.ingentaconnect.com/content/hsp/jpss/2015/00000009/00000003/art00001 (accessed on 10 March 2023).

Piper, Jason, and Alex Metcalfe. 2020. *Economic Crime in a Digital Age*. Ernst & Young Report. Available online: https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/assurance/assurance-pdfs/ey-economic-crime-digital-age.pdf (accessed on 6 January 2023).

PRISMA. 2023. Transparent Reporting of Systematic Reviews and Meta-Analyses. Available online: http://prisma-statement.org/ (accessed on 10 March 2023).

Prove. 2021. Risk Management: The Most Important Application of AI in the Fnancial Sector. Available online: https://www.prove.com/blog/risk-management-most-important-application-of-ai-in-financial-sector (accessed on 6 January 2023).

Puławska, Karolina, Wojciech Strzelczyk, and Arkadiusz Orzechowski. 2022. Cyber Insurance and Information Sharing as Prevention from Cyber-Attacks—Pilot Study. Available online: https://ssrn.com/abstract=4260821 (accessed on 10 March 2023).

Qin, Jing, and Qun Qin. 2021. Cloud platform for enterprise financial budget management based on artificial intelligence. *Wireless Communications and Mobile Computing* 2021: 8038433. [CrossRef]

Rahman, Md Sabizu, Yan Li, Mahabubur Rahman Miraj, Tariqul Islam, Md Kawsar Ahmed, and Mir Abdur Rob. 2022. Artificial Intelligence (AI) for Energizing the E-Commerce. Available online: https://www.researchgate.net/publication/359919374_Artificial_Intelligence_AI_for_Energizing_the_E-commerce/citations (accessed on 6 January 2023).

Raut, Jelena, Mitrović-Veljković Slavica, Melović Boban, and Vidicki Predrag. 2022. The influence of the entrepreneurial ecosystem on the initiation and development of innovation processes. *Serbian Journal of Engineering Management* 7: 8–13. [CrossRef]

Schanz, Kai-Uwe. 2018. Understanding and Addressing Global Insurance Protection Gaps. Available online: https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/understanding_and_addressing_global_insurance_protection_gaps.pdf (accessed on 10 March 2023).

Schatz, Daniel, Rabih Bashroush, and J. Julie Wall. 2017. Towards a More Representative Definition of. *Journal of Digital Forensics, Security and Law* 12: 8. [CrossRef]

Schroer, Alyssa. 2022. 28 Examples of AI in Finance: AI has Revolutionized the Finance Industry. Available online: https://builtin.com/artificial-intelligence/ai-finance-banking-applications-companies (accessed on 6 January 2023).

Serban, Iulian V., Chinnadhurai Sankar, Mathieu Germain, Saizheng Zhang, Zhouhan Lin, Sandeep Subramanian, Taesup Kim, Michael Pieper, Sarath Chandar, Nan Rosemary Ke, and et al. 2017. A deep reinforcement learning chatbot. *arXiv* arXiv:arXiv:1709.02349. [CrossRef]

Tsai, Sang-Bing, Youzhi Xue, Jianyu Zhang, Quan Chen, Yubin Liu, Jie Zhou, and Weiwei Dong. 2017. Models for forecasting growth trends in renewable energy. *Renewable and Sustainable Energy Reviews* 77: 1169–78. [CrossRef]

Xie, Xiaoying, Charles Lee, and Martin Eling. 2020. Cyber insurance offering and performance: An analysis of the U.S. cyber insurance market. *The Geneva Papers on Risk and Insurance—Issues and Practice* 45: 690–736. [CrossRef]

Xu, Xiaoling, and Jianghao Song. 2021. Enterprise financial leverage and risk assessment based on mobile payment under artificial intelligence. *Mobile Information Systems* 2021: 5468397. [CrossRef]

Yadav, Hitesha, Arpan K. Kar, and Smita Kashiramka. 2022. Artificial Intelligence Adoption for FinTech Industries—An Exploratory Study about the Disruptions, Antecedents and Consequences. In *The Role of Digital Technologies*. Edited by Savvas Papagiannidis, Eleftherios Alamanos, Suraksha Gupta, Yogesh K. Dwivedi, Matti Mäntymäki and Ilias O. Pappas. Cham: Springer, p. 13454. [CrossRef]

Yeoh, Peter. 2019. Rtificial intelligence: Accelerator or panacea for financial crime? *Journal of Financial Crime* 26: 634–46. [CrossRef]

Yu, Shi, Yuxin Chen, and Hussain Zaidi. 2020. A Financial Service Chatbot based on Deep Bidirectional Transformers. *arXiv* arXiv:2003.04987. Available online: https://arxiv.org/abs/2003.04987 (accessed on 6 January 2023). [CrossRef]

Zahariev, Andrey, Petko Angelov, and Silvia Zarkova. 2022. Estimation of Bank Profitability Using Vector Error Correction Model ans Support Vector Regression. *Economic Alternatives* 2: 157–70. [CrossRef]

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.