 doi:10.20944/preprints202108.0032.v1

Review

The impact of Artificial Intelligence on data system security: a literature review

Albérico Rosário [1] and Ricardo Raimundo [2,*]

[1]GOVCOPP, IADE – Universidade Europeia; alberico@ua.pt
[2] ISEC Lisboa, Instituto Superior de Educação e Ciências; ricardo.raimundo@iseclisboa.pt
*Correspondence: ricardo.raimundo@iseclisboa.pt

Abstract: Diverse forms of artificial intelligence (AI in further text) are at the forefront of triggering digital security innovations, based on the threats that are arising in this post COVID world. On the one hand, companies are experiencing difficulty in dealing with security challenges with regard to a variety of issues ranging from system openness, decision making, quality control and web domain, just to mention a few. On the other hand, in the last decade, research has focused on security capabilities based on tools such as platform complacency, intelligent trees, modeling methods and outage management systems, in an effort to understanding the interplay between AI and those issues. The dependence on the emergence of AI in running industries and shaping the education, transports and health sectors is now well known in literature. AI is increasingly employed in managing data security across economic sectors. Thus, a literature review of AI and system secu-rity within the current digital society is opportune. This paper aims at identifying research trends in the field through a Systematic Bibliometric Literature Review (LRSB) of research on AI and system security. The review entails 77 articles published in Scopus® database, presenting up-to-date knowledge on the topic. The LRSB results were synthesized across current research subthemes. Findings are presented. The originality of the paper relies on its LRSB method, together with extant review of articles that have not been categorized so far. Implications for future re-search are suggested.

Keywords: Artificial Intelligence; Securty; Security Of Data; Security Systems

1. Introduction

The assumption that the human brain may be deemed quite comparable to computers in some ways, offers the spontaneous basis for Artificial Intelligence (AI in further text), which is supported by psychology through the idea of humans and animals operating like machines that process information by devices of associative memory [1]. Nowadays, researchers are working on the possibilities of AI to cope with varying issues of systems security across diverse sectors. Hence, AI is commonly considered an interdisciplinary research area that attract considerable attention both in economics and social domains as it offers a myriad of technological breakthroughs with regard to systems security [2]. There is a universal trend of investing in AI technology to face security challenges of our daily lives, such as statistical data, medicine and transportation [3].

Some claim that specific data from key sectors have supported the development of AI, namely the availability of data from e-commerce [4], businesses [5] and government [6], which provided substantial input to ameliorate diverse machine learning solutions and algorithms, in particular with respect to systems security [7]. Additionally, China and Russia have acknowledged the importance of AI for systems security and competitiveness in general [8, 9]. Similarly, China has recognized the importance of AI in terms of housing security, aiming at becoming an authority in the field [10]. Those efforts are already being carried out in some leading countries, in order to profit the most from its substantial benefits [9]. In spite of the huge development of AI in the last few years, the discussion around

 doi:10.20944/preprints202108.0032.v1

the topic systems security is sparse [11]. Therefore, it is opportune to acquaint the last developments regarding the theme in order to map the advancements in the field and ensuing outcomes [12]. In the view of this, we intend to find out the principal trends of issues discussed on the topic these days in order to answer the main research question: What is the impact of AI on data system security?

The article is organized as follows. In section 2, we put forward diverse theoretical concepts related with AI in systems security. In section 3, we present the methodological approach. In section 4, we discuss the main fields of use of AI with regard to systems security, which came out from literature. Finally, we conclude this paper by suggesting implications and future research avenues.

2. Literature Trends: AI and Systems security

The concept of AI was introduced following the creation of the notion of digital computing machine in an attempt to ascertain whether a machine is able to 'think' [1], or if the machine can carry out humans' tasks [13]. AI is vast domain of Information and Computer Technologies (ICT in further text), which aims at designing systems that can operate autonomously, analogous to the individuals' decision making process [14].In terms of AI, a machine may learn from experience through processing immeasurable quantity of data, while distinguishing patterns in it, as in the case of Siri [15] and image recognition [16], technologies based on Machine Learning that is a subtheme of AI, de-fined as intelligent systems with the capacity to think and learn [1].

Furthermore, AI entails a myriad of related technologies, such as neural network [17] and machine learning [18], just to mention a few and we can identify some research areas of AI:

(I) Machine learning, is a myriad of technologies that allow computers to carry out algorithms based on gathered data and distinct orders, providing the machine the capabilities to learn without instructions from humans, adjusting its own algorithm to the situation, while learning and recoding itself, such as Google and Siri when performing distinct tasks ordered by voice [19]. As well, video surveillance that tracks unusual behavior [20].

(II) Deep Learning, constitutes the ensuing progress of machine learning, in which the machine carry out tasks directly from pictures, text and sound, through a wide set of data architecture that entails numerous layers, in order to learn and characterize data with several levels of abstraction imitating thus how the natural brain processes information [21]. This is illustrated for example in forming a certificate database structure of university Performance Key Indicators, in order to fix issues such as identity authentication [21].

(III) Neural Networks, is made of a pattern recognition system that machine / deep learning operates to perform learning from observational data, figuring out its own solutions such as a autosteering gear system with a fuzzy regulator, which enables to select optimal neural network models of the vessel paths, to obtain in this way control activity [22].

(IV) Natural Language processing machines, analyze language and speech as it is spoken, , resorting to Machine learning and natural language processing, such as developing a swarm intelligence and active system, while mounting friendly human computer interface software for users, to be implemented in educational and e-learning organizations [23].

(V) Expert systems, are made up of software arrangements that assist in achieving answers to distinct inquiries provided either by a customer or by another software set, in which expert knowledge is set aside in a particular area of the application that includes a reasoning component to access answers, in view of the environmental information and subsequent decision making [24].

Those subthemes of AI are applied to many sectors, such as health institutions, education, and management, through varying applications related to systems security. These

 doi:10.20944/preprints202108.0032.v1

abovementioned processes have been widely deployed to solve important secu-rity issues such as the following application trends (Figure 1):

a) Cyber security, in terms of computer crime, behavior research, access control and surveillance, as for example the case of computer vision, in which an algorithmic analyses images, CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) techniques, [6, 7, 12, 19, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38];

b) Information management, namely in supporting decision making, business strategy and expert systems for example by improving the quality of the relevant strategic deci-sions by analyzing big data, as well as in the management of the quality of complex objects [2, 4, 5, 11, 14, 24, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60];

c) Societies and institutions, regarding to computer networks, privacy and digitalization, legal and clinical assistance, for example in terms of legal support of cyber security, digital modernization, systems to support police investigations and the efficiency of technological processes in transport [8, 9, 10, 15, 17, 18, 20, 21, 23, 28, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73];

d) Neural networks, for example in terms of designing a model of human personality for use in robotic systems [1, 13, 16, 22, 74, 75].

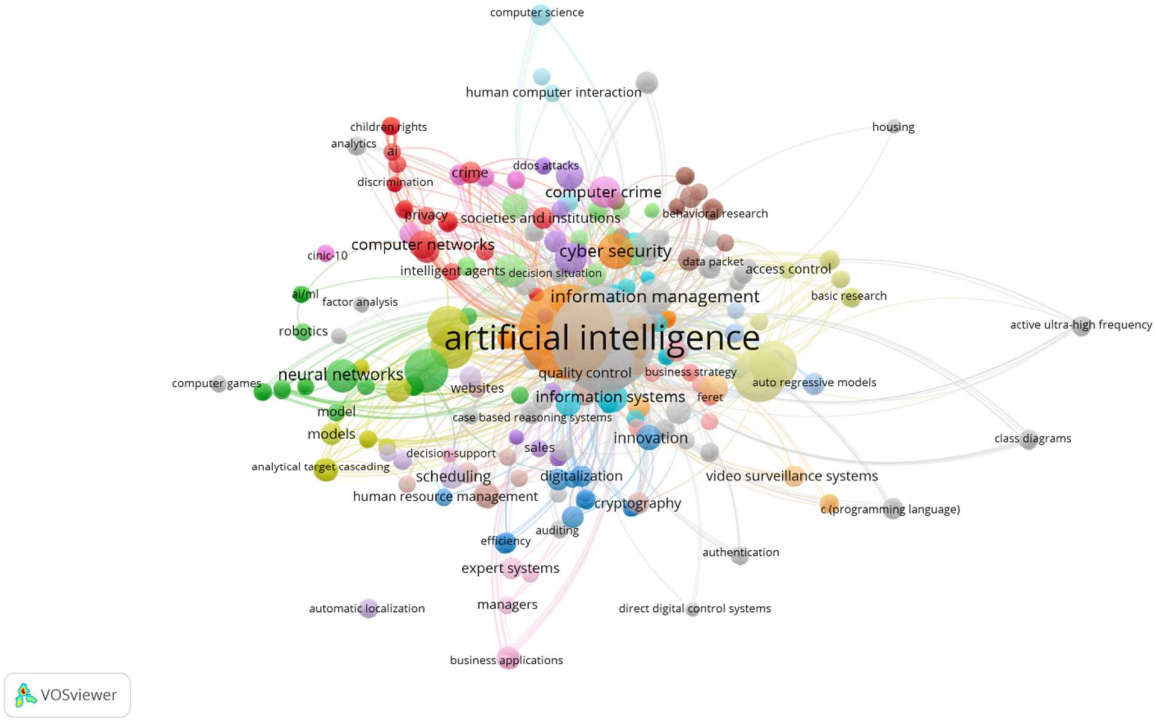

Figure 1. Subthemes / Network of all keywords of AI - Source: own elaboration.

Through these streams of research, we will explain how the huge potential of AI can be deployed, to over enhance systems security that are in use both in states and organizations, to mitigate risks and increase returns, while identifying, avert cyber at-tacks and determine the best course of action [19]. AI could even unveil to be more ef-fective than humans in averting potential threats by various security solutions such as redundant systems of video surveillance, VOIP voice network technology security strategies [36,76,77] and dependence upon diverse platforms for protection (platform complacency) [30].

 doi:10.20944/preprints202108.0032.v1

The design of the above mentioned conceptual and technological framework was not made randomly, as we did a preliminary search on Scopus with the keywords “Artificial Intelligence” and "Security".

2. Materials and Methods

We carried out a Systematic Bibliometric Literature Review (LRSB) of the "Impact of AI on Data System Security". The LRSB is a study concept that is based on a detailed, thorough study of the recognition and synthesis of information, being an alternative to traditional literature reviews, improving: (i) the validity of the review, providing a set of steps that can be followed if the study is replicated; (ii) accuracy, providing and demonstrating arguments strictly related to research questions; and (iii) the generalization of the results, allowing the synthesis and analysis of accumulated knowledge [78, 79, 80] . Thus, the LRSB is a "guiding instrument" that allows you to guide the review according to the objectives.

The study is performed following Raimundo and Rosário suggestions as follows: (i) definition of the research question; (ii) location of the studies; (iii) selection and evaluation of studies; (iv) analysis and synthesis; (v) presentation of results; finally (vi) discussion and conclusion of results. This methodology ensures a comprehensive, auditable, replicable review that answers the research questions.

The review was carried out in June 2021, with a bibliographic search in the Scopus database of scientific articles published until June 2021. The search was carried out in three phases: (i) using the keyword Artificial Intelligence "382,586 documents were ob-tained; (ii) adding the keyword "Security", we obtained a set of 15,916 documents; we lim-ited ourselves to Business, Management and Accounting 401 documents were obtained and finally (iii) exact keyword: Data security, Systems security a total of 77 documents were obtained (Table 1).

Table 1. Screening Methodology.

Database Scopus	Screening	Publications
Meta-search	keyword: Artificial Intelligence	382,586
Inclusion Criteria	keyword: Artificial Intelligence; Securty	15,916
	keyword: Artificial Intelligence; Securty Business, Management and Accounting	401
Screening	keyword: Artificial Intelligence; Securty Business, Management and Accounting Exact Keyword: Security Of Data; Security Systems Published until June 2021	77

Source: own elaboration.

The search strategy resulted in 77 academic documents. This set of eligible breakdowns was assessed for academic and scientific relevance and quality. Academic Documents, Conference Paper (43); Article (29); Review (3); Letter (1); and retracted (1).

Peer-reviewed academic documents on the impact of Artificial Intelligence on data system security were selected until 2020. In the period under re-view, 2021 was the year with the highest number of peer-reviewed academic documents on the subject, with 18 publications, with 7 publications already confirmed for 2021. Figure 2 reviews peer-reviewed publications published until 2021.

The publications were sorted out as follows: 2011 2nd International Conference On Artificial Intelligence Management Science And Electronic Commerce Aimsec 2011 Proceedings (14); Proceedings Of The 2020 IEEE International Conference Quality Management Transport And Information Security Information Technologies IT And Qm And Is 2020 (6); Proceedings Of The 2019 IEEE International Conference Quality Management Transport And Information Security Information Technologies IT And Qm And Is 2019

 doi:10.20944/preprints202108.0032.v1

(5); Computer Law And Security Review (4); Journal Of Network And Systems Management (4); Decision Support Systems (3); Proceedings 2021 21st Acis International Semi Virtual Winter Conference On Software Engineering Artificial Intelligence Networking And Parallel Distributed Computing Snpd Winter 2021 (3); IEEE Transactions On Engineering Management (2); Ictc 2019 10th International Conference On ICT Convergence ICT Convergence Leading The Autonomous Future (2); Information And Computer Security (2); Knowledge Based Systems (2); with 1 publication (2013 3rd International Conference On Innovative Computing Technology Intech 2013; 2020 IEEE Technology And Engineer-ing Management Conference Temscon 2020; 2020 International Conference On Technolo-gy And Entrepreneurship Virtual Icte V 2020; 2nd International Conference On Current Trends In Engineering And Technology Icctet 2014; ACM Transactions On Management Information Systems; AFE Facilities Engineering Journal; Electronic Design; Facct 2021 Proceedings Of The 2021 ACM Conference On Fairness Accountability And Transparency; HAC; ICE B 2010 Proceedings Of The International Conference On E Business; IEEE Engi-neering Management Review; Icaps 2008 Proceedings Of The 18th International Confer-ence On Automated Planning And Scheduling; Icaps 2009 Proceedings Of The 19th In-ternational Conference On Automated Planning And Scheduling;Industrial Management And Data Systems; Information And Management; Information Management And Com-puter Security; Information Management Computer Security; Information Systems Re-search; International Journal Of Networking And Virtual Organisations; International Journal Of Production Economics; International Journal Of Production Research; Journal Of The Operational Research Society; Proceedings 2020 2nd International Conference On Machine Learning Big Data And Business Intelligence Mlbdbi 2020; Proceedings Annual Meeting Of The Decision Sciences Institute; Proceedings Of The 2014 Conference On IT In Business Industry And Government An International Conference By Csi On Big Data Csibig 2014; Proceedings Of The European Conference On Innovation And Entrepreneur-ship Ecie; TQM Journal; Technology In Society; Towards The Digital World And Industry X 0 Proceedings Of The 29th International Conference Of The International Association For Management Of Technology Iamot 2020; Wit Transactions On Information And Communication Technologies).

We can say that in recent years there has been some interest in research on the impact of Artificial Intelligence on data system security.

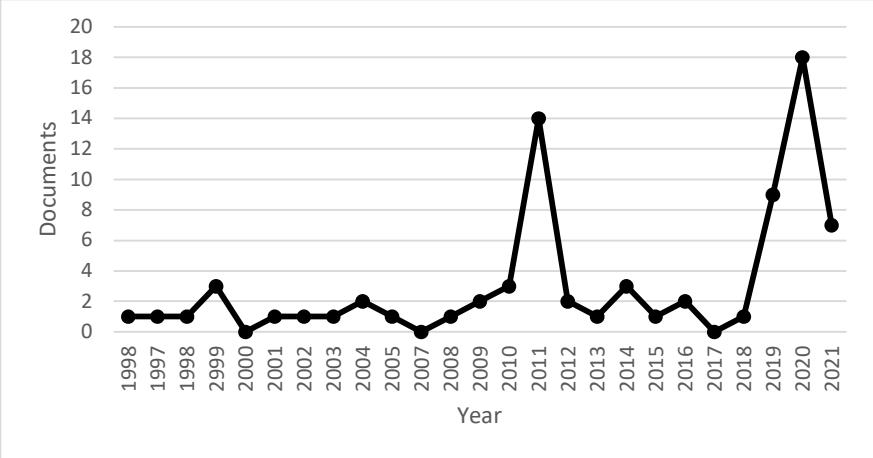

Figure 2. Documents by year. Source: own elaboration.

In Table 2 we analyze for the Scimago Journal & Country Rank (SJR), the best quartile and the H index by publication.

Information Systems Research is the most quoted publication with 3,510 (SJR), Q1 and H index 159.

There is a total of 11journals on Q1, 3 journals on Q2 and 2 journals, Q3 and 2 journal on Q4. Journals from best quartile Q1 represent 27% of the 41 journals titles; best quartile Q2 represents 7%, best quartile Q3 represents 5%, and finally, best Q4 represents 5% each of the titles of 41 journals. Finally 23 of the publications representing 56%, the data are not available.

As evident from Table 2, the significant majority of articles on of Artificial Intelligence on data system security rank on the Q1 best quartile index.

Table 2. Scimago journal & country rank impact factor.

Title	SJR	Best Quartile	H index
Information Systems Research	3,510	Q1	159
International Journal Of Production Economics	2,410	Q1	185
Information And Management	2,150	Q1	162
Knowledge Based Systems	1,590	Q1	121
Decision Support Systems	1,560	Q1	151
Industrial Management And Data Systems	0,990	Q1	103
Technology In Society	0,820	Q1	51
Computer Law And Security Review	0,820	Q1	38
Journal Of The Operational Research Society	0,750	Q1	108
IEEE Transactions On Engineering Management	0,700	Q1	92
ACM Transactions On Management Information Systems	0,600	Q1	29
Journal Of Network And Systems Management	0,490	Q2	35
Information And Computer Security	0,330	Q2	49
TQM Journal	0,540	Q2	67
IEEE Engineering Management Review	0,300	Q3	20
International Journal Of Production Research	0,270	Q3	19
International Journal Of Networking And Virtual Organisations	0,170	Q4	19
Electronic Design	0,100	Q4	7
Proceedings Of The European Conference On Innovation And Entrepreneurship Ecie	0,130	-*	6
Icaps 2008 Proceedings Of The 18th International Conference On Automated Planning And Scheduling	-*	-*	19
Wit Transactions On Information And Communication Technologies	-*	-*	13
Proceedings Annual Meeting Of The Decision Sciences Institute	-*	-*	9
Proceedings Of The 2014 Conference On IT In Business Industry And Government An International Conference By Csi On Big Data Csibig 2014	-*	-*	8
2nd International Conference On Current Trends In Engineering And Technology Icctet 2014	-*	-*	7
ICE B 2010 Proceedings Of The International Conference On E Business	-*	-*	6
AFE Facilities Engineering Journal	-*	-*	2
2011 2nd International Conference On Artificial Intelligence Management Science And Electronic Commerce Aimsec 2011 Proceedings	-*	-*	-*
Proceedings Of The 2020 IEEE International Conference Quality Management Transport And Information Security Information Technologies IT And Qm And Is 2020	-*	-*	-*
Proceedings Of The 2019 IEEE International Conference Quality Management Transport And Information Security Information Technologies IT And Qm And Is 2019	-*	-*	-*

 doi:10.20944/preprints202108.0032.v1

Proceedings 2021 21st Acis International Semi Virtual Winter Conference On Software Engineering Artificial Intelligence Networking And Parallel Distributed Computing Snpd Winter 2021	-*	-*	-*
Ictc 2019 10th International Conference On ICT Convergence ICT Convergence Leading The Autonomous Future	-*	-*	-*
2013 3rd International Conference On Innovative Computing Technology Intech 2013	-*	-*	-*
2020 IEEE Technology And Engineering Management Conference Temscon 2020	-*	-*	-*
2020 International Conference On Technology And Entrepreneurship Virtual Icte V 2020	-*	-*	-*
Facct 2021 Proceedings Of The 2021 ACM Conference On Fairness Accountability And Transparency	-*	-*	-*
HAC	-*	-*	-*
Icaps 2009 Proceedings Of The 19th International Conference On Automated Planning And Scheduling	-*	-*	-*
Information Management And Computer Security	-*	-*	-*
Information Management Computer Security	-*	-*	-*
Proceedings 2020 2nd International Conference On Machine Learning Big Data And Business Intelligence Mlbdbi 2020	-*	-*	-*
Towards The Digital World And Industry X 0 Proceedings Of The 29th International Conference Of The International Association For Management Of Technology Iamot 2020	-*	-*	-*

Note: *data not available. Source: own elaboration.

The subject areas covered by the 77 scientific documents were: Business, Management and Accounting (77); Computer Science (57); Decision Sciences (36); Engineering (21); Economics, Econometrics and Finance (15); Social Sciences (13); Arts and Humanities (3); Psychology (3); Mathematics (2); and Energy (1).

The most quoted article was "CCANN: An intrusion detection system based on combining cluster centers and nearest neighbors" from Lin, Ke and Tsai 290 quotes published in the Knowledge-Based Systems with 1,590(SJR), the best quartile (Q1) and with H index (121). The published article presents proposes a new resource representation approach, a cluster center and nearest neighbor approach.

In Figure 3 we can analyze the evolution of citations of documents published between 2010 and 2021, with a growing number of citations with an R2 of 0.45%.

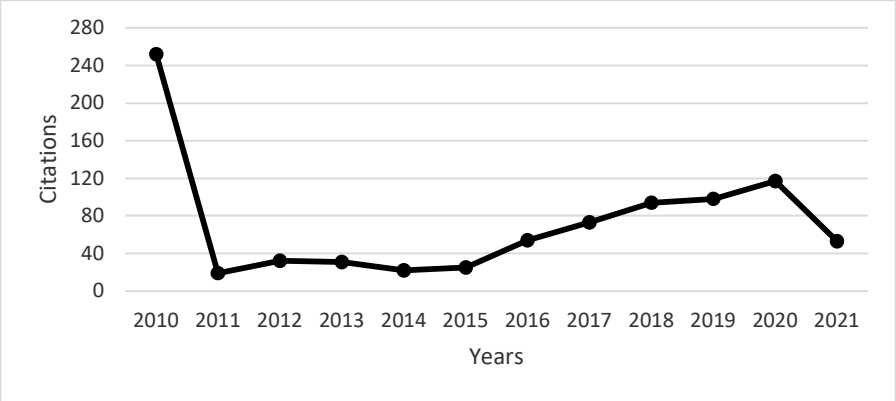

Figure 3. Evolution of citations between 2010 and 2021.Source: own elaboration

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 August 2021 doi:10.20944/preprints202108.0032.v1

The h-index was used to verify the productivity and impact of the documents, based on the largest number of documents included that had at least the same number of citations. Of the documents considered for the h-index, 11 have been cited at least 11 times.

In Appendix A, Table A1, citations of all scientific articles until 2021 are analyzed; 35 documents were not cited until 2021.

The h-index was used to verify the productivity and impact of the documents, based on the largest number of documents included that had at least the same number of citations. Of the documents considered for the h-index, 11 have been cited at least 11 times.

In Appendix A, Table A1, citations of all scientific articles until 2021 are analyzed; 35 documents were not cited until 2021.

Appendix B, Table B1, examines the self-quotation of documents until 2021, in which was identified self-quotation for a total of 16 self-quotations.

In Figure 4, a bibliometric analysis was performed to analyse and identify indicators on the dynamics and evolution of scientific information using the main keywords. The analysis of the bibliometric research results using the scientific software VOSviewe aims to identify the main keywords of research in “Artificial Intelligence” and "Security".

The linked keywords can be analysed in Figure 4, making it possible to clarify the network of keywords that appear together / linked in each scientific article, allowing to know the topics analysed by the research and to identify future research trends.

5. Discussion

By examining the selected pieces of literature, we have identified five principal areas that have been underscored and deserve further investigation with regard to cyber systems security: cyber security in general, business decision making, electronic commerce business, AI social applications and neural networks (figure 4). In this way, we present a detailed overview on the impacts of AI on each of those fields.

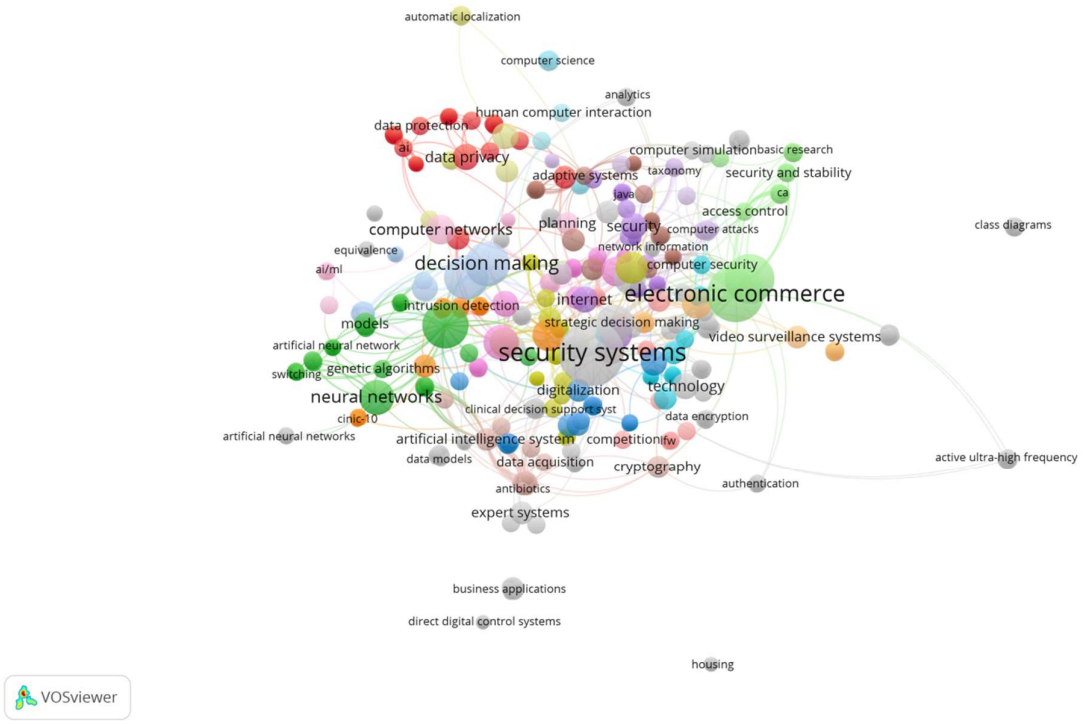

Figure 4. Network of Linked Keywords. Source: own elaboration.

 doi:10.20944/preprints202108.0032.v1

5.1. Cyber Security in general

There is a myriad of areas in where AI cyber security can be applied throughout social, private and public domains of our daily lives, from internet banking to digital signatures.

First, it has been discussed the possible decreasing of unnecessary leakage of accounting information [27], mainly through security drawbacks of VOIP technology in IP network systems and subsequent safety measures [77], which comprises a secure dynamic password used in the internet banking [29].

Second, it has been researched some computer user cyber security behaviors, which includes both a naïve lack of concern about the likelihood of facing security threats and dependence upon specific platforms for protection, as well as the dependence on the guidance from trusted social others [30], which has been partly resolved through a Mobile Agent (MA) management systems in distributed networks, while operating a model of open management framework that provides a broad range of processes to enforce security policies [31].

Third, AI cyber systems security always aim at achieving stability of the programming and analysis procedures by clarifying the relationship of code fault-tolerance programming with code security in detail, to strengthen it [33], offering an overview of existing cyber security tasks and roadmap [32].

Fourth, in this vein, numerous AI tools have been developed to achieve a multi stage security task approach for a full security life cycle [38]. New digital signature technology has been built, amidst the elliptic curve cryptography, of increasingly reliance [28]; new experimental CAPTCHA have been developed, through more interference characters and colorful background [8] to provide better protection against spam bots, allowing people with little knowledge of sign languages to recognize gestures on video relatively fast [70]; novel detection approach beyond traditional Firewall systems have been developed (e.g. cluster center and nearest neighbor - CANN) of higher efficiency for detection of attacks [71]; security solutions of AI for IoT (e.g. blockchain), due to its centralized architecture of security flaws [34]; and integrated algorithm of AI to identify malicious web domains for security protection of internet users [19].

In sum, AI has progressed lately by advancing in machine learning, with multilevel solutions to the security problems faced in security issues both in operating systems and networks, comprehending algorithms, methods and tools lengthily used by security experts for the better of the systems [6].

5.2. Business decision making

AI have an increasingly impact on systems security aimed at supporting decision making at management level. More and more, it is discussed expert systems that, along with the evolution of computers, are able to integrate systems into corporate culture [24]. Such systems are expected to maximize benefits against costs in situations where a decision making agent has to decide between a limited set of strategies of sparse information [14], while a strategic decision in a relatively short period of time is required demanded and of quality, for example by a intelligent analysis of big data [39].

Secondly, it has been adopted distributed decision models coordinated towards an overall solution, reliant on a decision support platform [40], either more of a mathematical / modeling support of situational approach to complex objects [41], or more of a web-based multi-perspective decision support system (DSS) [42].

Thirdly, the problem of software for the support of management decision was resolved by combining a systematic approach with heuristic methods and game-theoretic modeling [43] that, in the case of industrial security, reduces the subsequent number of incidents [44].

Fourthly, in terms of industrial management and ISO information security control, a semantic decision support system increases the automation level and support the

 doi:10.20944/preprints202108.0032.v1

decision-maker at identifying the most appropriate strategy against a modeled environment [45], while providing understandable technology that based the decisions and interact with the machine [46].

Finally, , with respect to team work, it AI validates a theoretical model of behavioral decision theory to assist organizational leaders in deciding on strategic initiatives [11], while allowing understanding who may have information that is valuable for solving a collaborative scheduling problem [47].

5.3. Electronic commerce business

The third research stream focuses on e-commerce solutions to improve its systems security. This AI research stream focuses on business, principally on security measures to electronic commerce (e-commerce), in order to avoid cyber-attacks, innovate, achieve information and ultimately get clients [5].

First, it has been built intelligent models around the factors that induce Internet users to make an on-line purchase, to build effective strategies [48], whereas it is discussed the cyber security issues by diverse AI models for controlling unauthorized intrusion [49], in particular in some countries such as China, to solve drawbacks in firewall technology, data encryption [4] and qualification [2].

Second, to adapt to the increasingly demanding environment nowadays of a world pandemic, in terms of finding new revenue sources for business [3] and restructure business digital processes to promote new products and services with enough privacy and manpower qualified accordingly and able to deal with the AI [50].

Third, to develop AI able to intelligently protect business either by a distinct model of Decision Trees amidst The Internet of Things (IoT) [51], or by ameliorating network management through Active Networks technology, of multi agent architecture able to imitate the reactive behavior and logical inference of a human expert [52].

Fourth, to re-conceptualize the role of AI within the proximity's spatial and non-spatial dimensions of a new digital Industry framework, aiming to connect the physical and digital production spaces both in the traditional and new technology based approaches (e.g. industry 4.0), promoting thus innovation partnerships and efficient technology and knowledge transfer [53]. In this vein, there is an attempt to move the management systems from a centralized to a distributed paradigm along the network and based on criteria such as for example the delegation degree [54] that inclusive allows the transition from industry 4.0 to industry 5.0i, through AI in the form of Internet of everything, multi-agent systems and emergent intelligence and enterprise architecture [58].

Fifth, in terms of manufacturing environments, following that networking paradigm, there is also an attempt in managing agent communities in distributed and varied manufacturing environments through an AI multi-agent virtual manufacturing system (e.g.MetaMorph) that optimizes real-time planning and security [55]. Also in manufacturing, smart factories have been built to mitigate security vulnerabilities of intelligent manufacturing processes automation by AI security measures and devices [56] as for example in the design of a mine security monitoring configuration software platform of a real-time framework (e.g. the device management class diagram)[26]. Smart buildings in manufacturing and non manufacturing environments have been adopted aiming at reducing costs, the height of the building and minimize the space required for users [57].

Finally, aiming at augmenting the cyber security of e-commerce and business in general, other projects have been put in place, such as Computer-assisted audit tools (CAATs), able to carry on continuous auditing, allowing auditors to augment their productivity, amidst the real time accounting and electronic data interchange [59] and a surge in the demand of high-tech / AI jobs [60].

 doi:10.20944/preprints202108.0032.v1

5.4. AI social applications

As seen, AI systems security can be widely deployed across almost all society domains, be in regulation, internet security, computer networks, digitalization, health and other numerous fields (see figure 4).

First, it has been an attempt to regulate cyber security, namely in terms of legal support of cyber security, with regard to the application of artificial intelligence technology [61], by an innovative and economical / political friendly way [9] and in fields such as infra structures, by ameliorating the efficiency of technological processes in transport, reducing for example the inter train stops [63] and education, by improving cyber security of university E-Gov, for example in forming a certificate database structure of university Performance Key Indicators [21] e-learning organizations by swarm intelligence [23] and acquanting the risk a digital campus will face according to ISO series standards and a criteria of risk levels [25]. while suggesting relevant solutions to key issues in its network information safety [12].

Second, some moral and legal issues have risen, in particular in relation with privacy, gender and childhood. Is the case of the ethical / legal legitimacy of publishing open source dual-purpose machine learning algorithms [18], the needed legislated framework comprising regulatory agencies and representatives of all stakeholder groups gathered around AI [68], the gendering issue of VPAs as female (e.g. Siri) as replicate normative assumptions about the potential role of women as secondary to men [15], the need of inclusion of communities to uphold its own Code [35]and the need to improve the legal position of people and children in particular that are exposed to AI mediated risk profiling practices [7, 69].

Third, the traditional industry also benefits with AI, given that it can improve for example the safety of coal mine, by analyzing the coal mine safety scheme storage structure, building data warehouse and analysis [64], ameliorating, as well, the security of smart cities and ensuing intelligent devices and networks, through AI frameworks (e.g. United Theory of Acceptance and Use of Technology- UTAUT) [65], housing [10] and building [66] security system in terms of energy balance (e.g. Direct Digital Control System), implying fuzzy logic as a non-precise program tool that allows the systems to function well [66], or even in terms of data integrity attacks to outage management system OMSs and ensuing AI means to detect and mitigate them [67].

Fourth, the citizens, in general, have reaped benefits from areas of AI such as police investigation, through expert systems that offer support in terms of profiling and tracking criminals based on machine-learning and neural network techniques to [17], video surveillance systems of real-time accuracy[76], resorting to models to detect moving objects keeping up with environment changes [36], of dynamical sensor selection in processing the image streams of all cameras simultaneously [37], whereas Ambient Intelligence (AmI) spaces, in where devices, sensors and wireless networks, combine data from a diverse sources and monitor user preferences and their subsequent results on users' privacy under a regulatory privacy framework [62].

Finally, AI has granted the society noteworthy progresses in terms of clinical assistance in terms of an integrated electronic health record system into the existing risk management software, to monitor sepsis at Intensive Care Unit (ICU) through a peer-to-peer VPN connection and with a fast and intuitive user interface [72]. As well, it has offered an AI organizational solution of innovative housing model that combines remote surveillance, diagnostics and the use of sensors and video, to detect anomalies on the behavior and health of the elderly [20], together with a case-based decision support system for the automatic real-time surveillance and diagnosis of health care associated infections, by diverse machine learning techniques [73].

 doi:10.20944/preprints202108.0032.v1

5.5. Neural networks

Neural networks, or the process through which machines learn from observational data, coming up with its own solutions, have been lately discussed over some stream of issues.

First, it has been argued that it is opportune to develop a software library for creating artificial neural networks for machine learning to solve non-standard tasks [74], along a decentralized and integrated AI environment that can accommodate video data storage and event-driven video processing, gathered from varying sources, such as video surveillance systems [16], which images could be improved through AI [75].

Second, such neural networks architecture has progressed into a huge number of neurons in the network, in which the devices of associative memory were designed with the number of neurons comparable to the human brain within supercomputers [1]. Subsequently, such neural networks can be modeled on the base of switches architecture to interconnect neurons and to store the training results in the memory, on the base of the genetic algorithms to be exported to other robotic systems: a model of human personality for use in robotic systems in medicine and biology [13].

Finally, neural network is quite representative of AI, in the attempt of, once trained in human learning and self learning, could operate without human guidance, as in the case of a current positioning vessel seaway systems, involving a fuzzy logic regulator, a neural network classifier enabling to select optimal neural network models of the vessel paths, to obtain control activity [22].

6. Conclusions

This piece of literature allowed illustrating the AI impacts on systems security, which influence our daily digital life, business decision making, e-commerce, diverse social and legal issues and on neural networks.

First, AI will potentially impact our digital and internet lives in the future, as the major trend is the emergence of increasingly new malicious threats from internet environment, likewise greater attention should be paid to cyber security. Accordingly, the progressively more complexity of business environment will demand, as well, more and more AI based support systems to decision making that enables management to adapt by a faster and accurate way, while requiring unique digital e-manpower.

Second, with regard to the e-commerce and manufacturing issues, principally amidst the world pandemic of COVID-19, it tends to augment exponentially, as already observed, which demands a subsequent progress with respect to cyber security measures and strategies. The same, regarding the social applications of AI that, following the increase of distance services, will also tend to adopt this model, applied to improved e-health, e-learning and e-elderly monitoring systems.

Third, subsequent divisive issues are being brought to the academic arena, which demands progress in terms of a legal framework, able to comprehend all the above mentioned issues, in order to assist the political decisions and match the expectations of citizens.

Lastly, it is inevitable a further progress in neural networks platforms, as it represents the cutting edge of AI, in terms of human thinking imitation technology, the main goal of AI applications.

To summarize, we have presented useful insights with respect to the impact of AI in systems security, while we illustrated its influence both on the people' service delivering, in particular in security domains of their daily matters, health / education and in business sector, through systems capable of supporting decision making. Also, we over-enhance the state of the art in terms of AI innovations applied to varying fields. Due to this scenario, we also suggest further research avenues to reinforce existing theories and developing new ones, in particular the deployment of AI technologies in Small Medium

Enterprises (SMEs), of sparse resources and from traditional sectors that constitute the core of intermediate economies and less developed and peripheral regions.

Author Contributions: R.R. and A.R. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: We would like to express our gratitude to the Editor and the Referees. They offered extremely valuable suggestions or improvements. The authors were supported by the GOVCOPP Research Unit of Universidade de Aveiro and ISEC Lisboa, Higher Institute of Education and Sciences.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

Appendix A

Table A1. Overview of document citations period ≤2010 to 2021.

Documents		≤2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	Total
An lntelligent Tree-Based lntrusion Detection Model for Cybe ...	2021	-	-	-	-	-	-	-	-	-	-	-	1	**1**
Trailblazing the Artificial lntelligence for Cybersecurity D ...	2020	-	-	-	-	-	-	-	-	-	-	-	1	**1**
Legal Remedies For a Forgiving Society: Children's rights, d ...	2020	-	-	-	-	-	-	-	-	-	-	-	**1**	**1**
The Challenges and Opportunities in the Digitalization ofCo ...	2020	-	-	-	-	-	-	-	-	-	-	-	**3**	**3**
New perspectives from technology adoption in senior cohousin ...	2020	-	-	-	-	-	-	-	-	-	-	-	**1**	**1**
From Alexa to Siri and the GDPR: The gendering ofVirtual Pe ...	2020	-	-	-	-	-	-	-	-	-	2	3	-	**5**
A Research on the Vulnerabilities of PLC using Search Engine	2019	-	-	-	-	-	-	-	-	-	1	-	-	**1**
lnformation Technology as the Basis for Transformation into ...	2019	-	-	-	-	-	-	-	-	-	-	4	3	**7**
Modeling the Effectiveness ofSolutions for Technogenic Safe ...	2019	-	-	-	-	-	-	-	-	-	-	6	1	**7**
he Neuron Network Model ofHuman Personality for …	2019	-	-	-	-	-	-	-	-	-	-	4		**4**
Regulatory alternatives for AI	2019	-	-	-	-	-	-	-	-	-	-	1	2	**3**
Malicious web domain identification using online…	2019	-	-	-	-	-	-	-	-	-	2	5	3	**10**

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 August 2021 doi:10.20944/preprints202108.0032.v1

Ontology-based information security compliance…	2018	-	-	-	-	-	-	-	-	-	1	4	-	**5**
Gesture-based animated CAPTCHA	2016	-	-	-	-	-	-	-	-	1		2	-	**3**
A case-based reasoning system for aiding detection and class ...	2016	-	-	-	-	-	-	-	11	7	8	9	4	**39**
CANN: An intrusion detection system based on combining clust...	2015	-	-	-	-	-	6	26	43	57	67	68	23	**290**
Real time BIG data analytic: Security concern and challenges ...	2014	-	-	-	-	-	-	2	1	-	1	2	-	**6**
Detecting and tracking of multi pie moving objects for intell ...	2014	-	-	-	-	-	-	-	2	1	4	-	-	**7**
Application of business intelligence to the power system…	2013	-	-	-	-	-	-	-	-	1	-	-	-	**1**
Generating Shareable Statistical Databases for Business Valu ...	2012	-	-	-	-	1	1	1	1	1	1	-	-	**6**
Study on security of electronic commerce information system	2011	-	-	-	-	-	-	-	-	-	-	1	-	**1**
The research on information safety problem of digital campus ...	2011	-	-	1	-	-	-	-	-	-	-	-	-	**1**
VOIP voice network technology security strategies	2011	-	-	1	-	-	-	-	1		1	-	-	**3**
Research on the Internet banking security based on dynamic p ...	2011	-	-	-	-	-	-	-	1	-	-	-	-	**1**
Analysis of coai mine safety monitoring data based …	2011	-	-	-	-	-	-	-	1	-	-	-	-	**1**
The improvement of digital signature algorithm based on…	2011	-	-	-	-	3	1	2	1	2	1	1	-	**11**
lntelligent mobile safety system to educational organization	2010	-	-	-	1	-	-	-	-	-	-	-	-	**1**
A web-based multi-perspective decision support system for in ...	2010	-	1	-	3	6	5	1	2	2	4	1	1	**27**
A generic analytical target cascading optimization system…	2010	2	3	-	3	3	1	1	5	2	2	1	-	**24**
A decision-theoretic approach to dynamic sensor selection in ...	2009	3	3	2	3	3	3	4	1	2	4	1	-	**29**
Privacy issues in Aml spaces	2009	-	-	-	-	-	-	-	-	-	1	1	-	**2**
Effective information value calculation for interruption man ...	2008	1	-	-	1	1	-	-	-	-	-	-	-	**3**
A logical architecture for aclive network management	2006	4	-	-	-	2	1	1	-	-	1	-	-	**9**

 doi:10.20944/preprints202108.0032.v1

Auditing in the e-commerce era	2004	10	2		5	3	3	1	4	2	3	2	1	**36**
Predictive model on the likelihood of online purchase in e-e ...	2002	1	-	-	-	-	-	-	-	-	-	-	-	**1**
Internet commerce security: lssues and models for contrai eh ...	2001	2	-	-	-	2	-	-	-	-	1	-	-	**6**
A survey of distributed enterprise network and systems manag ...	1999	42	2	2	2	1	3	1	1	2	-	-	-	**56**
An open secure Mobile Agent framework for systems…	1999	42	1	-	1	1	-	-	-	1	-	1	-	**36**
MetaMorph: An adaptive agent-based architecture for intellig ...	1999	117	5	8	6	3	6	4	-	5	2	2	-	**161**
AICAMS: Artificial intelligence crime analysis and managemen ...	1998	10	2		4	2	-	-	2	2	1	-	2	**27**
lmposing security constraints on agent-based decision suppor ...	1997	21	-	-	-	-	1	1	1		2	-	-	**26**
An empirical study ofthe use ofbusiness expert systems	1988	7	-	-	-	-	-	-	-	-	-	-	-	**7**
	Total	**252**	**19**	**32**	**31**	**22**	**25**	**54**	**73**	**94**	**98**	**117**	**53**	**870**

Appendix B

Table A2. - Overview of document self-citation period ≤2010 to 2020.

Documents		≤2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	Total
Trailblazing the Artificial lntelligence for Cybersecurity D ...	2020	-	-	-	-	-	-	-	-	-	-	-	1	**1**
The Challenges and Opportunities in the Digitalization ofCo ...	2020	-	-	-	-	-	-	-	-	-	-	-	1	**1**
lnformation Technology as the Basis for Transformation into ...	2019	-	-	-	-	-	-	-	-	-	-	2	-	**2**
Modeling the Effectiveness ofSolutions for Technogenic Safe ...	2019	-	-	-	-	-	-	-	-	-	-	1	1	**2**
Malicious web domain identification using online credibility ...	2019	-	-	-	-	-	-	-	-	-	2	2	2	**4**
Gesture-based animated CAPTCHA	2016	-	-	-	-	-	-	-	-	-	-	1	-	**1**
A case-based reasoning system for aiding detection and class ...	2016	-	-	-	-	-	-	-	-	1	-	-	-	**1**
The research on information safety problem of digital campus ...	2011	-	-	-	-	-	-	-	-		-	-	1	**1**

A generic analytical target cascading optimization system...	2010		1	3	1		1	2	1	1	-	-	-	**10**
A decision-theoretic approach to dynamic sensor selection in ...	2009	1	1	-	-	-	-	-	-	1	-	-	-	**3**
A logical architecture for aclive network management	2006	1	-	-	-	1	1	-	-	-	-	-	-	**3**
Auditing in the e-commerce era	2004		-	-	-	1		-	-	-	-	-	-	**1**
MetaMorph: An adaptive agent-based architecture for intellig ...	1999	7	-	-	-	-	-	-	-	-	-	-	-	**7**
AICAMS: Artificial intelligence crime analysis and managemen ...	1998	12	-	-	-	-	1	1	-	-	1	-	-	**15**
An empirical study ofthe use ofbusiness expert systems	1988	11	-	-	-	-	-	-	1	-	-	-	-	**12**
	Total	**32**	**2**	**3**	**1**	**2**	**3**	**3**	**2**	**3**	**3**	**6**	**6**	**64**

References

1. Sheptunov, S.A.; Sukhanova, N.V. The problems of design and application of switching neural networks in creation of artificial intelligence. Paper presented at the *Proceedings of the 2020 IEEE International Conference "Quality Management, Transport and Information Security, Information Technologies", IT and QM and IS 2020,* **2020**, 428-431.
2. Kim, M.S. The design of industrial security tasks and capabilities required in industrial site. Paper presented at the *Proceedings - 2021 21st ACIS International Semi-Virtual Winter Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, SNPD-Winter,2021,* **2021**, 218-223.
3. Melville, N.; McQuaid, M. Generating shareable statistical databases for business value: Multiple imputation with multimodal perturbation. *Information Systems Research,* **2012,** *23*(2), 559-574.
4. Zhu, F.; Li, G. Study on security of electronic commerce information system. Paper presented at the *2011 2nd International Conference on Artificial Intelligence, Management Science and Electronic Commerce, AIMSEC 2011 - Proceedings,* **2011,** 1546-1549.
5. Hu, X.; Wang, K. Bank financial innovation and computer information security management based on artificial intelligence. Paper presented at the *Proceedings - 2020 2nd International Conference on Machine Learning, Big Data and Business Intelligence, MLBDBI 2020,* **2020,** 572-575.
6. Singh, J. Real time BIG data analytic: Security concern and challenges with machine learning algorithm. Paper presented at the *Proceedings of the 2014 Conference on IT in Business, Industry and Government: An International Conference by CSI on Big Data, CSIBIG 2014,* **2014**.
7. Choi, H.; Young, K.J. Practical approach of security enhancement method based on the protection motivation theory. Paper presented at the *Proceedings - 2021 21st ACIS International Semi-Virtual Winter Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, SNPD-Winter 2021,* **2021,** 96-97.
8. Sun, Y.; Men, T.; Huang, G. Analysis and design of China's E-bank CAPTCHA. Paper presented at the *WIT Transactions on Information and Communication Technologies,* **2014**, *61,* 1343-1350.
9. Popkova, E.; Alekseev, A.N.; Lobova, S.V.; Sergi, B.S. The theory of innovation and innovative development. AI scenarios in russia. *Technology in Society,* **2020**, *63*.
10. Zhong, X.; Ji, G. RETRACTED ARTICLE: Research on the development measures of housing security system. *2011 2nd International Conference on Artificial Intelligence, Management Science and Electronic Commerce, AIMSEC 2011 - Proceedings,* **2011**, 586-588.
11. Workman, M. Validation of a biases model in strategic security decision making. *Information Management & Computer Security,* **2012**, *20*(2), 52-70.
12. Li, F. The research on information safety problem of digital campus network. Paper presented at the *2011 2nd International Conference on Artificial Intelligence, Management Science and Electronic Commerce, AIMSEC 2011 - Proceedings,* **2011,** 828-831.
13. Sukhanova, N.V.; Sheptunov, S.A.; Glashev, R.M. The neuron network model of human personality for use in robotic systems in medicine and biology. Paper presented at the *Proceedings of the 2019 IEEE International Conference Quality Management, Transport and Information Security, Information Technologies IT and QM and IS 2019,* **2019,** 11-16.

14. Ekenberg, L.; Danielson, M.; Boman, M. Imposing security constraints on agent-based decision support. *Decision Support Systems,* **1997,** *20*(1), 3-15.
15. Loideain, N.N.; Adams, R. From alexa to siri and the GDPR: The gendering of virtual personal assistants and the role of data protection impact assessments. *Computer Law and Security Review,* **2020,** *36*
16. Khelvas, A.; Demyanova, D.; Gilya-Zetinov, A.; Konyagin, E.; Khafizov, R.; Pashkov, R. Adaptive distributed video surveillance system. Paper presented at the *2020 International Conference on Technology and Entrepreneurship - Virtual, ICTE-V 2020*, **2020**.
17. Brahan, J.W.; Lam, K.P.; Chan, H.; Leung, W. AICAMS: Artificial intelligence crime analysis and management system. *Knowledge-Based Systems,* **1998,** *11*(5-6), 355-361.
18. Nikolskaia, K.; Naumov, V. Ethical and legal principles of publishing open source dual-purpose machine learning algorithms. Paper presented at the *Proceedings of the 2020 IEEE International Conference "Quality Management, Transport and Information Security, Information Technologies", IT and QM and IS 2020,* **2020,** 56-58.
19. Hu, Z.; Chiong, R.; Pranata, I., Bao, Y.; Lin, Y. Malicious web domain identification using online credibility and performance data by considering the class imbalance issue. *Industrial Management and Data Systems,* **2019,** *119*(3), 676-696.
20. Angioni, M.; Musso, F. New perspectives from technology adoption in senior cohousing facilities. *TQM Journal,* **2020,** *32*(4), 761-777.
21. Huang, L.; Ye, C. -. Research of secure university E-government based on PKI. Paper presented at the *2011 2nd International Conference on Artificial Intelligence, Management Science and Electronic Commerce, AIMSEC 2011 - Proceedings,* **20117**, 174-7177.
22. Sedova, N.A.; Sedov, V.A.; Dudareva, O.V.; Bazhenov, R.I.; Lavrushina, E. G. An autosteering gear system with a fuzzy regulator adjusted by a neural network. Paper presented at the *Proceedings of the 2019 IEEE International Conference Quality Management, Transport and Information Security, Information Technologies IT and QM and IS 2019,* **2019,** 197-202.
23. Chen, L. -. Intelligent mobile safety system to educational organization. Paper presented at the *ICE-B 2010 - Proceedings of the International Conference on e-Business,* **2010,** 55-62.
24. Beheshtian-Ardekani, M.; Salchenberger, L.M. An empirical study of the use of business expert systems. *Information and Management,* **1988,** *15*(4), 183-190.
25. Lv, X. Information security risk evaluation for e-campus. Paper presented at the *2011 2nd International Conference on Artificial Intelligence, Management Science and Electronic Commerce, AIMSEC 2011 - Proceedings,* **2011,** 2153-2154.
26. An, W.; Wang, H. Design for the configuration software of coalmine security monitoring. Paper presented at the *2011 2nd International Conference on Artificial Intelligence, Management Science and Electronic Commerce, AIMSEC 2011 - Proceedings,* **2011,** 2947-2950.
27. He, Q.; Chen, G. Research of security audit of enterprise group accounting information system under internet environment. Paper presented at the *2011 2nd International Conference on Artificial Intelligence, Management Science and Electronic Commerce, AIMSEC 2011 - Proceedings,* **2011,** 516-519.
28. Zhang, Q.; Li, Z.; Song, C. The improvement of digital signature algorithm based on elliptic curve cryptography. Paper presented at the *2011 2nd International Conference on Artificial Intelligence, Management Science and Electronic Commerce, AIMSEC 2011 - Proceedings,* **2011,** 1689-1691.
29. Xiong, Y. Research on the internet banking security based on dynamic password. Paper presented at the *2011 2nd International Conference on Artificial Intelligence, Management Science and Electronic Commerce, AIMSEC 2011 - Proceedings,* **2011,** 4746-4749.
30. Stafford, T.F. Platform-dependent computer security complacency: The unrecognized insider threat. *IEEE Transactions on Engineering Management,* **2021**
31. Bellavista, P.; Corradi, A.; Stefanelli, C. An open secure mobile agent framework for systems management. *Journal of Network and Systems Management,* **1999,** *7*(3), 323-339.
32. Samtani, S.; Kantarcioglu, M.; Chen, H. Trailblazing the artificial intelligence for cybersecurity discipline: A multi-disciplinary research roadmap. *ACM Transactions on Management Information Systems,* **2020,** *11*(4).
33. Gao, L.; Zheng, D. -. Analysis on code stability and fault tolerance. Paper presented at the *2011 2nd International Conference on Artificial Intelligence, Management Science and Electronic Commerce, AIMSEC 2011 - Proceedings,* **2011,** 155-159.
34. Dhieb, N.; Ghazzai, H.; Besbes, H.; Massoud, Y. Scalable and secure architecture for distributed IoT systems. Paper presented at the *2020 IEEE Technology and Engineering Management Conference, TEMSCON 2020,* **2020**.
35. Cheong, M.; Leins, K.; Coghlan, S. Computer science communities: Who is speaking, and who is listening to the women? using an ethics of care to promote diverse voices. Paper presented at the *FAccT 2021 - Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency,* **2021,** 106-115.
36. Prakash, U.M.; Thamaraiselvi, V. G. Detecting and tracking of multiple moving objects for intelligent video surveillance systems. Paper presented at the *2nd International Conference on Current Trends in Engineering and Technology, ICCTET 2014,* **2014,** 253-257.

37. Spaan, M.T.J.; Lima, P.U. A decision-theoretic approach to dynamic sensor selection in camera networks. Paper presented at the *ICAPS 2009 - Proceedings of the 19th International Conference on Automated Planning and Scheduling,* **2009,** 297-304.
38. Lei, X. Cyber-security analysis for process control oriented information system. Paper presented at the *2011 2nd International Conference on Artificial Intelligence, Management Science and Electronic Commerce, AIMSEC 2011 - Proceedings,* **2011,** 289-292.
39. Cherviakov, L.M.; Sheptunov, S.A.; Oleynik, A V.; Bychkova, N.A. Digitalization of quality management of the strategic decision-making process. Paper presented at the *Proceedings of the 2020 IEEE International Conference "Quality Management, Transport and Information Security, Information Technologies", IT and QM and IS 2020,* **2020,** 193-196.
40. Qu, T.; Huang, G.Q.; Zhang, Y.; Dai, Q.Y. A generic analytical target cascading optimization system for decentralized supply chain configuration over supply chain grid. *International Journal of Production Economics,* **2010,** *127*(2), 262-277.
41. Titov, A.A.; Rogov, A.A. Mathematical support of modeling methods in quality management problems of complex system and processes. Paper presented at the *Proceedings of the 2019 IEEE International Conference Quality Management, Transport and Information Security, Information Technologies IT and QM and IS 2019,* **2019,** 308-311.
42. El-Gayar, O.F.; Fritz, B.D. A web-based multi-perspective decision support system for information security planning. *Decision Support Systems,* **2010,** *50*(1), 43-54.
43. Tagiltseva, J.A.; Kuzina, E.L.; Bortnik, O.A.; Shlikov, E.E.; Magomedov, S.S.; Vasilenko, M.A.; Drozdov, N.A. Modeling the effectiveness of solutions for technogenic safety in the electrical industry. Paper presented at the *Proceedings of the 2019 IEEE International Conference Quality Management, Transport and Information Security, Information Technologies IT and QM and IS 2019,* **2019,** 100-105.
44. Jacome-Grajales, N.; Escobedo-Briones, G.; Roblero, J.; Arroyo-Figueroa, G. Application of business intelligence to the power system process security. Paper presented at the *2013 3rd International Conference on Innovative Computing Technology, INTECH 2013,* **2013,** 258-262.
45. Fenz, S.; Neubauer, T. Ontology-based information security compliance determination and control selection on the example of ISO 27002. *Information and Computer Security,* **2018,** *26*(5), 551-567.
46. Canal, G.; Borgo, R.; Coles, A.; Drake, A.; Huynh, D.; Keller, P., . . . Sklar, E. I. Building trust in human-machine partnerships. *Computer Law and Security Review,* **2020**, *39*.
47. Sarne, D.; Grosz, B.J.; Owotoki, P. Effective information value calculation for interruption management in multi-agent scheduling. Paper presented at the *ICAPS 2008 - Proceedings of the 18th International Conference on Automated Planning and Scheduling,* **2008,** 313-321.
48. Lee, P. -.; Yau, C. -.; Tan, K. -.; Chee, M. -. Predictive model on the likelihood of online purchase in e-commerce environment. Paper presented at the *Proceedings - Annual Meeting of the Decision Sciences Institute,* **2002,** 569-574.
49. Hansen, J.V. Internet commerce security: Issues and models for control checking. *Journal of the Operational Research Society,* **2001,** *52*(10), 1159-1164.
50. Almeida, F.; Duarte Santos, J.; Augusto Monteiro, J. The challenges and opportunities in the digitalization of companies in a post-COVID-19 world. *IEEE Engineering Management Review,* **2020,** *48*(3), 97-103.
51. Al-Omari, M.; Rawashdeh, M.; Qutaishat, F.; Alshira'H, M.; Ababneh, N. An intelligent tree-based intrusion detection model for cyber security. *Journal of Network and Systems Management,* **2021,** *29*(2).
52. Gaglio, S.; Gatani, L.; Lo Re, G.; Urso, A. (2006). A logical architecture for active network management. *Journal of Network and Systems Management, 14*(1), 127-146.
53. Stathaki, C.; Xenakis, A.; Skayannis, P.; Stamoulis, G. Studying the role of proximity in advancing innovation partnerships at the dawn of industry 4.0 era. Paper presented at the *Proceedings of the European Conference on Innovation and Entrepreneurship, ECIE, , 2020-September,* **2020,** 651-658.
54. Martin-Fiatin, J. -.; Znaty, S.; Hubaux, J. -. A survey of distributed enterprise network and systems management paradigms. *Journal of Network and Systems Management,* **1999,** *7*(1), 9-26.
55. Maturana, F.; Shen, W.; Norrie, D. H. MetaMorph: An adaptive agent-based architecture for intelligent manufacturing. *International Journal of Production Research,* **1999,** *37*(10), 2159-2173.
56. Lee, T.; Kim, S.; Kim, K. A research on the vulnerabilities of PLC using search engine. Paper presented at the *ICTC 2019 - 10th International Conference on ICT Convergence: ICT Convergence Leading the Autonomous Future,* **2019,** 184-188.
57. Haddlesey, P. Artificial intelligence. *HAC,* (NOVEMBER/DECEMBER), **2003,** 18-20.
58. Martynov, V. V.; Shavaleeva, D. N.; Zaytseva, A. A. Information technology as the basis for transformation into a digital society and industry 5.0. Paper presented at the *Proceedings of the 2019 IEEE International Conference Quality Management, Transport and Information Security, Information Technologies IT and QM and IS 2019,* **2019,** 539-543.
59. Zhao, N.; Yen, D. C.; Chang, I. -. Auditing in the e-commerce era. *Information Management and Computer Security,* **2004,** *12*(5), 389-400.
60. Schneiderman, R. Outsourcing: How safe is your job? *Electronic Design,* **2004,** *52*(10), 48-54.
61. Kseniia, N.; Minbaleev, A. Legal support of cybersecurity in the field of application of artificial intelligence technology. Paper presented at the *Proceedings of the 2020 IEEE International Conference "Quality Management, Transport and Information Security, Information Technologies", IT and QM and IS 2020,* **2020,** 59-62.

62. Kafeza, E.; Kafeza, I. Privacy issues in AmI spaces. *International Journal of Networking and Virtual Organisations,* **2009,** *6*(6), 634-650.
63. Efimova, O. V.; Baboshin, E. B.; Igolnikov, B. V.; Dmitrieva, E. I. Promising digital solutions for the efficient technological and managerial processes on transport. Paper presented at the *Proceedings of the 2020 IEEE International Conference "Quality Management, Transport and Information Security, Information Technologies", IT and QM and IS 2020,* **2020,** 92-95.
64. Zhao, W.; Li, S. Analysis of coal mine safety monitoring data based on column-oriented database. Paper presented at the *2011 2nd International Conference on Artificial Intelligence, Management Science and Electronic Commerce, AIMSEC 2011 - Proceedings,* **2011,** 1920-1922.
65. Grandhi, L. S.; Grandhi, S.; Wibowo, S. A security-UTAUT framework for evaluating key security determinants in smart city adoption by the australian city councils. Paper presented at the *Proceedings - 2021 21st ACIS International Semi-Virtual Winter Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, SNPD-Winter 2021,* **2021,** 17-22.
66. Saya, W. P. The building of intelligence. *AFE Facilities Engineering Journal,* **2005,** *32*(5), 7-11.
67. Hong, T.; Hofmann, A. Data integrity attacks against outage management systems. *IEEE Transactions on Engineering Management,* **2021**.
68. Clarke, R. Regulatory alternatives for AI. *Computer Law and Security Review,* **2019,** *35*(4), 398-409.
69. La Fors, D. K. Legal remedies for a forgiving society: Children's rights, data protection rights and the value of forgiveness in AI-mediated risk profiling of children by dutch authorities. *Computer Law and Security Review,* **2020,** *38*.
70. Shumilov, A.; Philippovich, A. Gesture-based animated CAPTCHA. *Information and Computer Security,* **2016,** *24*(3), 242-254.
71. Lin, W. -.; Ke, S. -.; Tsai, C. -. CANN: An intrusion detection system based on combining cluster centers and nearest neighbors. *Knowledge-Based Systems,* **2015,** *78*(1), 13-21.
72. de Fátima Stankowitz, R.; Salvação, P. M.; Lima, E. B.; de Medeiros Amaro, M. L.; Morales, H. M. P. Proposal of an electronic health record integrated to an artificial intelligence system for early detection of sepsis. Paper presented at the *Towards the Digital World and Industry X.0 - Proceedings of the 29th International Conference of the International Association for Management of Technology, IAMOT 2020,* **2020,** 918-927.
73. Gómez-Vallejo, H. J.; Uriel-Latorre, B.; Sande-Meijide, M.; Villamarín-Bello, B.; Pavón, R.; Fdez-Riverola, F.; Glez-Peña, D. A case-based reasoning system for aiding detection and classification of nosocomial infections. *Decision Support Systems,* **2016,** *84*, 104-116.
74. Maksim, B.; Pavel, W.; Irina, V.; Mikhail, S.; Margarita, C. Development of a software library for game artificial intelligence. Paper presented at the *Proceedings of the 2020 IEEE International Conference "Quality Management, Transport and Information Security, Information Technologies", IT and QM and IS 2020,* **2020,** 188-192.
75. Sharif, M.; Kausar, A.; Park, J.; Shin, D. R. Tiny image classification using four-block convolutional neural network. Paper presented at the *ICTC 2019 - 10th International Conference on ICT Convergence: ICT Convergence Leading the Autonomous Future,* **2019,** 1-6.
76. Yang, Y. -.; Zeng, H.; Li, Z. -. The video surveillance system based on DSP and wireless network. Paper presented at the *2011 2nd International Conference on Artificial Intelligence, Management Science and Electronic Commerce, AIMSEC 2011 - Proceedings,* **2011,** 2657-2659.
77. Zhang, Y.; Huang, H. VOIP voice network technology security strategies. Paper presented at the *2011 2nd International Conference on Artificial Intelligence, Management Science and Electronic Commerce, AIMSEC 2011 - Proceedings,* **2011,** 3591-3594.
78. Rosário, A.; Vilaça F.; Raimundo, R.; Cruz, R.; literature review on health knowledge management in the last 10 years (2009-2019). *Electronic Journal of Knowledge Management*. **2021**, 18(3), 338-355.
79. Raimundo, R; Rosário, A. Blockchain system in the higher education. *European Journal of Investigation in Health, Psychology and Education*. **2021**, 11(1), 276-293.
80. Rosário, A.; Fernandes, F.; Raimundo, R.; Cruz, R. Determinants of Nascent Entrepreneurship Development. In Carrizo Moreira, A.; Dantas, J. G. (Ed.), Handbook of Research on Nascent Entrepreneurship and Creating New Ventures, **2021**, (pp. 172-193). IGI Global.