 doi:10.20944/preprints202110.0312.v1

Review

Cybersecurity in the Internet of Things in Industrial Management

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

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

Abstract: Nowadays, people live amidst the smart home domain, business opportunities in the industrial smart city and health care, though, along with concerns about security. Security is central for IoT systems to protect sensitive data and infrastructure, whilst security issues become increasingly expensive, in particular in Industrial Internet of Things (IIoT) domains. Nonetheless, there are some key challenges for dealing with those security issues in IoT domains: Applications operate in distributed environments such as Blockchain, varied smart objects are used, and sensors are limited in what comes to machine resources. In this way, traditional security does not fit in IoT systems. In this vein, the issue of cyber security has become paramount to the Internet of Things (IoT) and Industrial Internet of Things (IIoT) in mitigating cyber security risk for organizations and end users. New cyber security technologies / applications present improvements for IoT security management. Nevertheless, there is a gap on the effectiveness of IoT cyber risk solutions. This review article discusses the, trends around opportunities and threats in cyber security for IIoT.

Keywords: Cyber Security; Internet of Things

1. Introduction

The internet of things (IoT) aims at integrating the digital and physical universes into a distinct system, thus providing major business opportunities for several sectors such as industry, tourism and energy. It has created a new paradigm in which a net-work of machines and devices capable of communicating and collaborating with each other are driving new processes. However, IoT is fragile in terms of many security is-sues that are frequently highly demanding due to its complex context and a vast num-ber of tools, which present flaws in terms of resources [1]. IoT is a system where the Internet is linked to the physical world through sensors [2] and can be deemed as the management of a network of devices, home appliances and vehicles of the IoT that is challenging due to the dynamic nature of the linkage between devices, actors and re-source constraints [3, 4] involving hardware, software, sensors, and connectivity which allows them to connect, gather and exchange data [5]. Central for for IoT is the "smart factory", in which comprehends diverse elements: person, process, intelligent object and technological ecosystem [6]. IoT embraces traditional Internet connectivity to likewise traditionally non physical devices such as cars and electric tools, just to mention a few. As well, IoT is strongly related to manufacturing, in order to produce high quality products at low costs by putting together Industrial Internet of Things (IIoT), cloud computing and big data analytics [7], including robots [8].

The IoT has therefore become prevalent over diverse sectors, with the Inter-net-of-Battlefield-Things (IoBT), or the Internet-of-Vehicles (IoV) [3, 9] along with its security issues, contributing therefore to the increasing of cyber attacks. Therefore, lately, it has been a concern with cyber security in this domain, amid a lack of policy direction and lack of understanding of user values related to cyber security in terms of the IoT, while policy has not been guided by key stakeholder values [10].

Cyber security copes with the protection of electronics, software and data, along with the procedures by which systems are accessed. In general, security objectives comprise privacy, in terms of information not inappropriately disclosed to unauthor-ized devices or individuals to be modified or destroyed [11, 12]. In this way, due to the countless connected devices that based IoT, society is becoming also increasingly vul-nerable to cyber attacks, such as Denial-of-service attacks, direct access attacks [13] performed for example by hackers and insiders [14, 15]. Technology is increasingly more central in our daily lives, which means that also cybercrime and cyber security tools evolve concomitantly [16, 17], comprising the whole manufacturing sector [18] that needs to invest in cyber security counter measures, while new cyber security technologies are emerging for IoT cyber security management [19].

Furthermore, cyber attacks on smart grids, as key infrastructure components are particularly vulnerable and of greater costs, impacting severely on the safety condition of citizens and governments [13], in which there is a growing concern on cyber securi-ty and the lack of effective counter measures e.g. cyber security professionals [20]. For instance, China is building a new Cyber Security Law and strategy [21], while Healthcare is currently a hot topic because there is an abundance of critical data, de-fenses are in average weak in hospitals, where patient lives and trust is at risk [22].

As previous pieces of literature focus on the technical features of IoT cyber secu-rity, there is a knowledge gap on frameworks to address the complex cyber security is-sues in IoT. This article presents thus a literature review on IoT security technologies and cyber risk management in industry.

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

2. Literature Review: key concepts

Due to the characteristics of both cyber attacks and the IoT systems, it is necessary to understand the discussed concepts before move forward to the major current trends on the issue.

2.1. Cyber security

Cyber security turned out to be a major worry, as we know that most of our usual objects can be connected to internet, which is paramount in our daily lives. In so, if it can be connected, therefore, can be accessed. The primary concern for cyber security relies thus upon intrusion detection [23], in where physical or cloud computer activi-ties are monitored through analysis of system vulnerabilities and activity patterns [24]. The attacks could assume the form of, for example, Denial-Delay-of-Service (DDoS) [13], malicious IPs [25] and Data Manipulation [26], with ensuing outcomes, such as loss of information, operational losses and health damage [22, 27].

2.2. Internet of Things

As already aforementioned, the Internet of Things (IoT) can be described as a new theme that encapsulates both the prevailing internet and the physical artifacts [1]. We can mention, for instance the 'smart home' [11] referring to home automation, manu-facturing systems as the industrial process, and health in terms of hospital automation [11]

In this vein, IoT heavily augments the multiple gadgets and connected devices on our lives, for instance in smart grids [11] and in transportation through Electric Vehi-cles (EV) [3]. Thus, the internet technology, although presenting countless advantages, poses serious threats, as well [28]. IoT applications cover consequently a wide range of artifacts, from a smart home [25] to a huge smart factory [6], of smart grids [13]. In all mentioned cases, the correspondent devices are complemented with wireless interfaces of wireless

 doi:10.20944/preprints202110.0312.v1

sensor network (WSN) that constitutes a key IoT technology [1, 2] to the wide stream of IoT systems, in particular 'smart grid', 'internet of thing' , 'manufac-turing systems', 'smart cities', and 'cloud computing in transport and smart homes [6, 8, 11, 25]

In the one hand, in the case of Smart Home, it is advisable to protect sensors identities from being recognized through wireless communication environment networks, while keeping the software up to date, from trustable vendors and cloud providers [1].in the other hand, in the case of smart cities, to which many population will tend to migrate, IoT offer multiple services such as smart parking, environmental, waste, wa-ter and traffic management and energy consumption monitoring, through operations that comprehend across IoT, its energy and architecture efficiency, mitigating its en-vironmental effects, always aware of its context interplay [26, 29].

2.3. The Industrial Internet of Things (IIoT)

IIoT presents diverse nuances that differentiate it from traditional IoT. While the IoT operates in domestic environs, IIot operates in industrial environ. In this way, it copes with, for example, the optimization of supply chains, as to say, IIoT equals In-dustry 4.0 [30], which means a shared term for technologies and theories of value chain organization [18, 31]. Industry 4.0 presents a modular structure, through which computers monitor and manage smart factories and its ensuing physical processes [32], creating a digital copy of the physical processes, while making decentralized de-cisions [33]. Along the process, computer systems interact one to another and people at once [30].

Also, both organizational and inter organizational services can be provided to ac-tors of the supply chain, interconnected objects, managed and accessed through data mining processes like Blockchain can be partly accessed and function as sensors and are enabled to interact with other devices [34, 35]. Such system, made up of smart ar-tifacts within the IoT system demands minimal or none human action to exchange and produce data, often assisted by Artificial Intelligence mechanisms [36]. To summarize, the IIoT major concerns include reduce material and energy consumption, better managing the temporal dimensions of security in terms of 'intrusion detection', cloud computing and the interface between supply chain management and marketing pro-cesses; and better managing the complexity of infrastructures in terms of number of entry points [11, 18, 32, 34, 37, 38].

The IIoT assembles therefore, both cyber security and IoT concerns in general. It focus on integrity, in which data is protected from modification by unauthorized party and authentication, in which the data source is verified as the pretended identity [39]; privacy, in which users' identities are non-traceable from their behaviors [40] confi-dentiality, in which information is made unintelligible to unauthorized entities, and Availability, in which the system services are available only for legitimate users [41].

IIoT faces thus important challenges in terms of, for example, operations in de-centralized environs such as Blockchain systems [42, 43] and varying nature of smart artifacts [44]. Also, it is noteworthy to mention the sparse computational resources and power available to the diverse sensors that result in insufficient traditional security measures [9, 45]. Those aforementioned issues augment the chances of cyber attacks to IoT systems, namely plants, transportation and household appliances [9], demanding substantial improvement in terms of authentication from remote systems, encryption from new sensors, and web interface and computer software for intrusion detection [46]. Additionally, the more IoT innovation, the more development in wireless tech-nologies, as well, such as the 5G, optimized well beyond voice and data, offering thus a vast array of opportunities [15, 47].

The literature review we present in this piece of literature, also suggest a set of security solutions for cordless sensor networks with respect to IoT [48, 49, 50]. In par-ticular, in terms of network computing, of decentralized architectures, made up of countless objects [15], such as the Blockchain [25] and cloud computing systems that ease network management and configuration [51, 52], ameliorating thus the IoT secu-rity [53], through

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 October 2021 doi:10.20944/preprints202110.0312.v1

sensors that optimize the sending of data, avoiding thus the redun-dancy in the wireless channels by systems such as big data that improve networking [18, 30, 54, 55].

The design of the conceptual and technological framework for this piece of litera-ture was not made randomly, as we did a preliminary search on Scopus with the key-words “Internet of Things” and "Cyber Security", which results are presented and dis-cussed in the following sections.

2. Materials and Methods

This investigation uses a Systematic Review of Bibliometric Literature (LRSB) as proposed by Rosário and Raimundo [56], Raimundo and Rosário [57], Rosário et al., [58]. This qualitative approach analyzes and synthesizes documents on cybersecurity in the internet of things in industrial management that clearly indicate determining contexts the purpose of research through rigorous and precise design. Summarizing and combined relevant studies, thus expanding usable knowledge in decision-making and strategies. The main advantage of qualitative research is to allow the collection and analysis of data of cybersecurity factors in the internet of things in industrial management. LRSB are designed to be methodical, explicit and playable. This type of study provides guidance for the development of sketches, indicating new methods for future investigations and identifies which research methods have been used. With this methodology, it intended to build new knowledge about the context of cybersecurity in the internet of things in industrial management.

The LRSB process was carriers out, divided into 3 phases and 6 stages (Table 1), as proposed by Rosário and Raimundo (2021), Raimundo and Rosário (2021), Rosário et al., (2021).

Table 1. Systematic LRSB process.

Phase	Step	Description
Exploration	Step 1	problem of research
	Step 2	search of appropriate literature
	Step 3	the critical precision of the chosen studies
	Step 4	synthesis of data from individual sources
Interpretation	Step 5	reports and recommendations
Communicatio	Step 6	presentation of the LRSB report

The database of indexation of scientific and/or academic documents was SCOPUS, the most important peer review of the scientific and/or academic environment. With nearly 19,500 titles from more than 5,000 international publishers, covering the cov-erage of 16,500 peer-reviewed journals in the scientific and/or academic fields.

However, we consider that the study has the limitation of considering only the SCOPUS indexing database, excluding the other scientific and academic indexing da-tabases.

Bibliographic research includes peer-reviewed scientific and/or academic documents published by September 2021. The initial search involved the keyword "Cyber Security" and "Internet of Things" to track summaries, titles and keywords. 15,748 documents were identified using the keyword "Cyber Security" reduced to 1,316, add-ing the keyword "Internet of Things". The research was later limited to the research area "Business, Management and Accounting" to caution that only the most relevant research (Table 2).

Finally, content techniques and thematic analysis were users to recognize, analyze and report the various documents proposed by Rosário and Raimundo (2021), Raimundo and Rosário (2021), Rosário et al., (2021).

Table 2. Screening Methodology.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 October 2021 doi:10.20944/preprints202110.0312.v1

Database Scopus	Screening	Publications
Meta-search	keyword: Cyber Security	15,748
First Inclusion Criterion	keyword: Cyber Security, Internet of Things	1,316
Second Inclusion Criterion	keyword: Cyber Security, Internet of Things Subject area Business, Management and Accounting	60
Tracking	keyword: Cyber Security, Internet of Things Subject area Business, Management Published until September 2021	

Source: own elaboration.

The 60 scientific and/or academic documents indexed in SCOPUS are later ana-lyzers in a narrative and bibliometric way to deepen the content and possible deriva-tion of common themes that respond directly to the question of research (Rosário & Raimundo, 2021, Raimundo & Rosário, 2021, Rosário et al., 2021).

Of the 60 documents selected, 28 documents are conference paper; 24 articles; 4 reviews; 3 books; and 1 book chapter and short survey.

Publication distribution

Peer-reviewed articles on the topic be period 2014-2021. The year 219 were the one with the most peer-reviewed publications on the subject, reaching 15.

Figure 1 summarizes the published peer-reviewed literature for the 2014-2021 period. The publications were sorted out as follows: With 4 documents Computer Law And Security Review and Proceedings IEEE 2018 International Congress On Cyber-matics 2018 IEEE Conferences On Internet Of Things Green Computing And Commu-nications Cyber Physical And Social Computing Smart Data Blockchain Computer And Information Technology Itings Greencom Cpscom Smartdata Blockchain CIT 2018; with 3 documents International Journal Of Recent Technology And Engineering; with 2 (2019 IEEE Technology And Engineering Management Conference Temscon 2019; Annual Conference On Innovation And Technology In Computer Science Educa-tion Iticse; Journal Of Network And Systems Management; Journal Of Telecommuni-cations And The Digital Economy; Proceedings Of The International Conference On Industrial Engineering And Operations Management); and the other publications with one document eachInterest in the subject has varies over time.

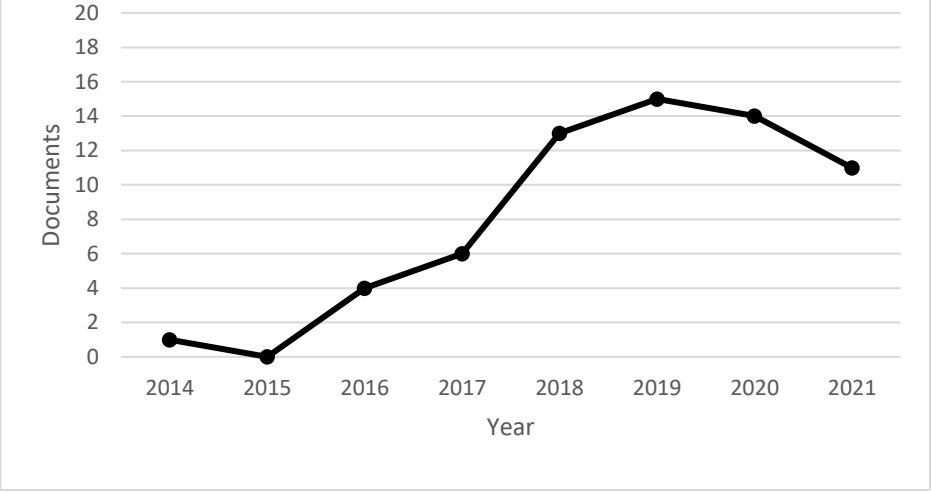

Figure 1. Documents by year. Source: own elaboration.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 October 2021 doi:10.20944/preprints202110.0312.v1

In Table 3 we analyze for the Scimago Journal & Country Rank (SJR), the best quartile and the H index by publication.

International Journal Of Information Management is the most quoted publication with 2,770 (SJR), Q1 and H index 114.

There is a total of 7 journals on Q1, 4 journals on Q2 and 7 journals, Q3 and 5 journal on Q4. Journals from best quartile Q1 represent 15% of the 48 journals titles; best quartile Q2 represents 8%, best quartile Q3 represents 15%, and finally, best Q4 represents 10% each of the titles of 48 journals. Finally, 25 of the publications repre-senting 52%, the data are not available.

As evident from Table 3, the significant majority of articles on of Cybersecurity in the Internet of Things in Industrial Management on the Q1 best quartile index.

Table 2. Scimago journal & country rank impact factor.

Title	SJR	Best Quartile	H index
International Journal Of Information Management	2,770	Q1	114
Journal Of Cleaner Production	1,940	Q1	200
Computer Law And Security Review	0,820	Q1	38
Technology In Society	0,820	Q1	51
Business Process Management Journal	0,670	Q1	81
Advances In Production Engineering And Management	0,620	Q1	18
ACM Transactions On Management Information Systems	0,600	Q1	29
Journal Of Network And Systems Management	0,490	Q2	35
International Journal Of Automotive Technology And Management	0,380	Q2	22
Foresight	0,370	Q2	30
Entrepreneurial Business And Economics Review	0,330	Q2	11
Vision	0,310	Q3	9
IEEE Engineering Management Review	0,300	Q3	20
Managerial Finance	0,270	Q3	39
International Journal Of Business Information Systems	0,260	Q3	26
Academy Of Entrepreneurship Journal	0,210	Q3	12
Journal Of Telecommunications And The Digital Economy	0,200	Q2	6
Logforum	0,200	Q3	4
International Journal Of Business Analytics	0,160	Q4	9
International Journal Of Computing And Digital Systems	0,150	Q4	6
International Journal Of Technology Intelligence And Planning	0,130	Q4	15
Economist United Kingdom	0,100	Q4	9
Petroleum Economist	0,100	Q4	4
Annual Conference On Innovation And Technology In Computer Science Education Iticse	0,260	-*	23
Proceedings 16th IEEE Acis International Conference On Computer And Information Science Icis 2017	0,210	-*	17
12th Aeit International Annual Conference Aeit 2020	0,190	-*	9

Proceedings Of The Summer School Francesco Turco	0,150	-*	9
Proceedings Of The International Conference On Industrial Engineering And Operations Management	0,130	-*	9
Proceedings Of The International Conference On Electronic Business Iceb	0,120	-*	7
2017 IEEE Technology And Engineering Management Society Conference Temscon 2017	0,210	-*	6
2019 IEEE Technology And Engineering Management Conference Temscon 2019	0,150	-*	4
Ictc 2019 10th International Conference On ICT Convergence ICT Convergence Leading The Autonomous Future	0,120	-*	3
2018 IEEE Technology And Engineering Management Conference Temscon 2018	0,120	-*	3
Idimt 2018 Strategic Modeling In Management Economy And Society 26th Interdisciplinary Information Management Talks	0,100	-*	3
International Journal Of Recent Technology And Engineering	0	-*	20
Contributions To Management Science	0	-*	14
Proceedings IEEE 2018 International Congress On Cybermatics 2018 IEEE Conferences On Internet Of Things Green Computing And Communications Cyber Physical And Social Computing Smart Data Blockchain Computer And Information Technology Ithings Greencom Cpscom Smartdata Blockchain CIT 2018	-*	-*	-*
2020 IEEE Technology And Engineering Management Conference Temscon 2020	-*	-*	-*
2020 International Conference On Technology And Entrepreneurship Virtual Icte V 2020	-*	-*	-*
Artificial Intelligence Techniques For A Scalable Energy Transition Advanced Methods Digital Technologies Decision Support Tools And Applications	-*	-*	-*
How To Compete In The Age Of Artificial Intelligence Implementing A Collaborative Human Machine Strategy For Your Business	-*	-*	-*
Innovation Technology In Smart Cities	-*	-*	-*
Joint 13th Ctte And 10th Cmi Conference On Internet Of Things Business Models Users And Networks	-*	-*	-*
Proceedings 18th IEEE International Conference On Machine Learning And Applications Icmla 2019	-*	-*	-*
Proceedings 2019 IEEE 5th International Conference On Collaboration And Internet Computing Cic 2019	-*	-*	-*
Proceedings 2020 IEEE International Conference On Blockchain Blockchain 2020	-*	-*	-*

 doi:10.20944/preprints202110.0312.v1

Proceedings 2021 21st Acis International Semi Virtual Winter Conference On Software Engineering Artificial Intelligence Networking And Parallel Distributed Computing Snpd Winter 2021	-*	.*	-*
Proceedings Of International Conference On Research Innovation Knowledge Management And Technology Application For Business Sustainability Inbush 2020	-*	-*	-*

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

The subject areas covered by the 60 scientific articles were: Business, Management and Accounting (60); Computer Science (31); Engineering (25); Decision Sciences (23); Social Sciences (14); Economics, Econometrics and Finance (7); Energy (5); Medicine ; Environmental Science (3); Mathematics; and Physics and Astronomy.

The most quoted article was "Blockchain technology innovations" with 155 quotes published in the 2017 IEEE Technology and Engineering Management Society Conference, TEMSCON 2017, 0,210 (SJR), not yet assigned quartile and with H index (6).

The published article focuses the study demonstrates the use of Blockchain tech-nology in various industrial applications.

In Figure 2 we can analyze the evolution of citations of articles published between 2014 and 2021. The number of quotes shows a positive net growth with an R2 of 80% for the period 2014-2021, with 2020 reaching 217 citations.

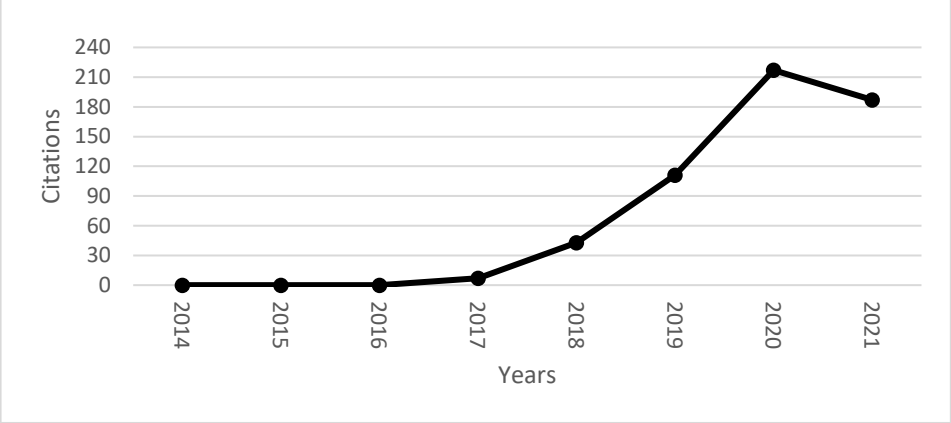

Figure 2. Evolution of citations between 2014 and 2020. (Source: own elaboration)

The h-index was used to ascertain the productivity and impact of the published work, based on the largest number of articles included that had at least the same number of citations. Of the documents considered for the h-index, 10 have been cited at least 10 times.

In appendix I, the citations of all scientific articles from the 2014 to 2021 period are analyzed, with a total of 568 citations, of the 60 publications 19 were not cited. Appendix II examines the self-citation of the document during the period 2014 to 2021, 20 documents were self-cited 48 times, the article 20 years of scientific evolution of cyber security: A scienc... by Furstenau et al. (2020) published in the Proceedings of the International Conference on Industrial Engineering and Operations Management was cited 10 times.

In Figure 3, a bibliometric study was performed to examine the development of scientific information by the main keywords. The study of bibliometric outputs by the scientific software VOSviewe, aims at identifying the main research keywords "Cyber Security", "Internet of Things".

The research relied upon the studied articles on consumer marketing strategy on e-commerce in the last decade. The correlated keywords can be viewed in Figure 4 al-lowing to making clear the network of keywords that appear together / linked in each scientific

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 October 2021 doi:10.20944/preprints202110.0312.v1

article, as well as knowing the topics studied to identify future research trends. Also, Figure 5 illustrates co-citations with a unit of analysis of cited references.

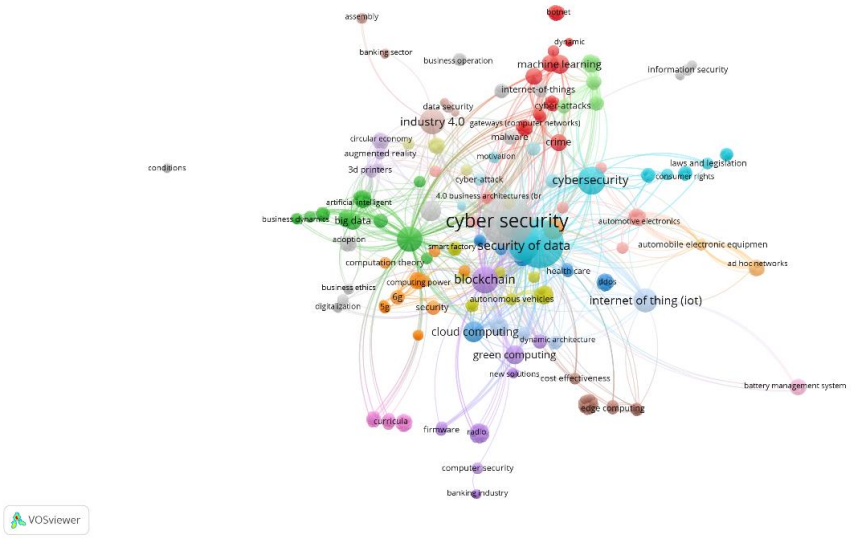

Figure 3. Network of all keywords. Source: own elaboration.

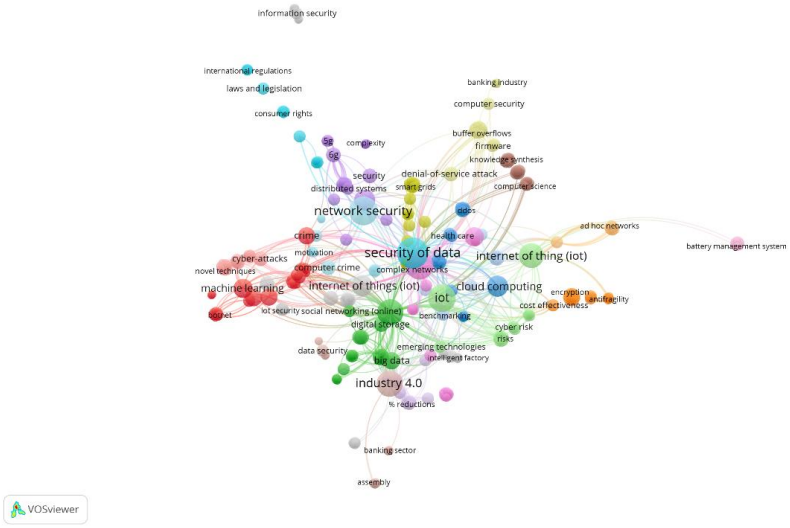

Figure 4. Network of Linked Keywords. Source: own elaboration.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 October 2021 doi:10.20944/preprints202110.0312.v1

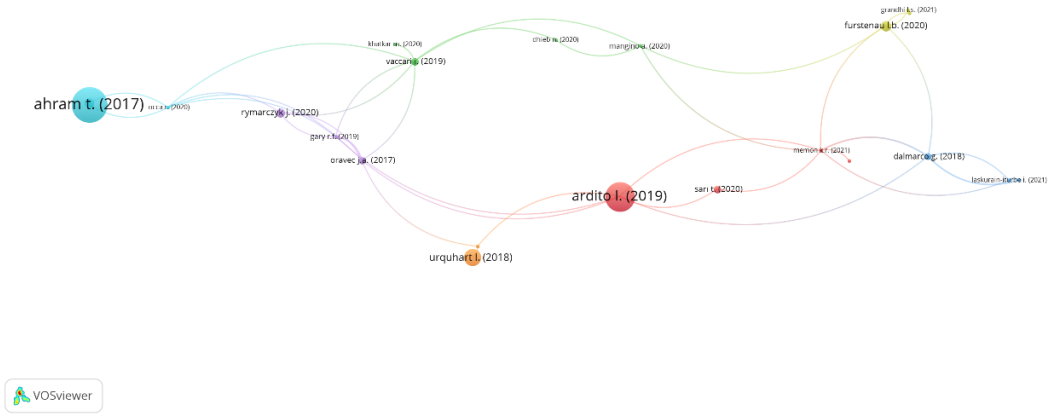

Figure 5. Networks of co-citation. Source: own elaboration.

4. Discussion

The aforementioned topics related with cyber security in IIoT emerge in literature under distinct subthemes, such as, for example, machine learning and cloud compu-ting, through several applications related to security. These abovementioned concepts have been widely deployed to solve important issues and highlight principal authors, particularly Ahram [20] and Ardito [32] (figure 5). Also, the key themes that under-score the current debate are illustrated above (Figure 3 and Figure 4):

4.1. Cyber Security

Cyber security, as already discussed, has focused primarly on securing distinct data form phisical and cloud threats. It deals with the cyber security threats to digital infrastructure and are a concern for the mantenance of business growth amidst a sce-nario of changing technologies of social, mobility, analytics and cloud (SMAC) do-mains and internet of things (IOTs), demanding the validation of new cyber security capabilities [39]. It focus on the users' susceptibility to cyberattack, how different fac-tors e.g. users' competence to deal with online threats, mediate the relationship in IoT [40]; it elicit major significant threat drivers and identify emerging technologies, e.g. encryption and blockchain that are likely to have an impact on defense and attack ca-pabilities in cyber security [16].

Existent literature identify, as well, major platforms that could accommodate smart objects, such as smart home systems that are platforms for connecting sensors, which are consequently exposed to identity theft and need to be protected [1]; the is-sues of securing automated power consumption units, implemented by smart system technology in an environment controlled by IoT [41]; and review the most critical technologies, best practices, policies and security frameworks in different countries; relevant government, industry, civil society and academia [59]. Finally, some pieces of literature examine whether Cyber Security Law is justified, analyzing some countries e.g. China that need a cyber security regime [21];

4.2. Machine Learning

Closely related to cyber security is the issue of machine learning that includes artificial inteligence. This theme is focused on intelligence for energy management, in-cluding production systems, its cyber security in industry 4.0 and internet of things [49]. It is much centred on the interplay between the feature selection and the inter-pretation steps in a machine learning workflow, aiming at intrusion detection in IoT networks [24]. It

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 October 2021 doi:10.20944/preprints202110.0312.v1

resorts often to artificial intelligence (AI) techniques for recognizing a cyberattack in internet-connected systems domains such as smartphones or robotic factories and on what to do in the appearance of an incident through data mining ap-proaches, in which AI will improve cyber counter measures [8]. Others intend to in-volve AI in business, assisting in adopting a strategy that is rational, relevant, and practical, across enterprise functions including disruptive technologies such as IoT, Blockchain, and cloud computing [36];

4.3. Internet of Things (IoT)

IoT is central on this debate and its influence extends to industry (IIoT), network and cloud computing. This issue has shed light on the implementation of intrusion de-tection systems, able to protect data and physical devices, through for instance AI that allows an intelligent intrusion detection model to detect threats, through Decision Trees for network intrusion detection [23]. It operates also to household participants, to obtain control over the intelligent IoT agents operating in their personal spheres [60]; to executives, in providing businesses with an approach for securing an enterprise by a dynamic architecture of Extended Risk-Based Approach on Cloud and IoT [61]; and in general to all virtually paperless work environments [62], aiming at threats re-lated with distributed denial of service (DDoS) on power grids and hacking of indus-trial control systems (ICS) along with the ensuing regulatory responses [13].

IoT theory also search for solutions related with how supply chains as a whole may benefit from the adoption of 4.0 technologies, delivering the flexible response customers want, and benefit from big data, cloud computing and cyber security by an improved communication system [30]. For example, it aims at analyzing devices and network security, while considering different scenarios involving varying attackers intending to destroy the IoT wireless network [17], whereas applying learning curves to major global cyber-attacks [42].

Other stream of literature explores what technologies are being deployed and where the organizational risk is being considered within the organization, buildign a risk model to deal with AI, IoT and distributed ledger [43], while offered a detailed study of trust management models to enforce different security measures in IoT sys-tem, ensuring thus safety to connected devices [44]. Including technologies such as Augmented reality (AR), a concept that connects the real world to the virtual world, to develop guidelines, to industry 4.0. [31], to tourism, in integrating business and key performance metrics to build a strategy for smart tourism [63].

It is notewhorty to mention the case of Electric Vehicles (EVs) cybersecurity issues in identifying the key matters, of the overall EVs that have been developed, but do not address the requirements of cybersecurity (e.g. the EV battery stacks) [3], on networks [4] and suggest strategies the auto industry might pursue in this subject to face cyber-security threats [28]. In the same vein, others detail the security vulnerabilities of un-manned ships, subsequent defense strategies and ensuing countermeasures [55], while signaling vulnerabilities of wireless systems of software radios [45].

To summarize, as the Smart Devices are growing in number, there is a corre-sponding growth in risks, both to the user and to the internet as a whole by the hacking threats [54], whereas there is a lack of policy direction, user values on cybersecurity are misunderstood and there is a lack of clarity as to how IoT public policy should be de-veloped, as for instance being guided by stakeholder values [10]. Moreover, a new paradigm of proactive antifragility for cyber defence approaches is demanded in IoT, for instance in distributed computing paradigms of high complexity, beyond tradition-al cyber defence .e.g. the Internet of Battle Things (IoBT) [9], able to cope with novel threats [53].

Finally, others, propose solutions to new wireless challenges such as the 6G, shifting the paradigm "from Internet of Things (IoT) to Internet of Intelligence (IoI)", to provide connectivity, while mantaining the ability to process knowledge and make de-cisions autonomously [47]. Developing thus a novel methodology for fingerprinting IoT devices, by building data-driven techniques rooted in machine learning methods, which allows to

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 October 2021 doi:10.20944/preprints202110.0312.v1

unveil compromised IP addresses throughout diverse geographical areas [5]. Also it focus on the issue of distributed denial of service (DDoS) scope, in terms of classifications and opportunities for attacks, particularly in the health sector, of limited security [22], while examining the changing legal environment in the IoT regulatory context [48];

4.4. Industry 4.0 (IIoT)

Industry 4.0 is another important subtheme related with IoT. It is also known as Industrial Internet of Things (IIoT). Some literature investigate the influence of critical technologies such as Artificial Intelligence, Big Data and Virtual Augmented Reality on the circular economy e.g. recycling and reduction of waste and emissions, which con-firms the importance of Industry 4.0 for improving circularity [18]. Others enhance the impact of those digital technologies on e-finance, an opportunity to change business models, for example through AI [27]; develop such digital technologies for managing the interface between supply chain management and marketing processes in sustain-ing supply chain management marketing (SCM-M) integration [32]; focus on the oil and gas industry in terms of treaths on the migration of sensitive business data to the cloud digital platforms in industrial processes, which include decision-making pro-cesses and procedures [33] and the increasing of entry points for organizations to de-fend from threats [34].

Other stream of literature spots the research gaps in industry 4.0, using an open (Google) internet-based research search engine (OIBRSE) to acquire the digital object identifiers and universal resource locators if the DOI non-exists with research articles [53], namely regarding current debates around, for example the issue of Smart factory, which bases on ICT technology, used to drive down manufacturing costs and time, while security vulnerabilities must be reduced [6]. Moreover, with regard to this sort of critical infrastructures, securing electro-energy platforms represents an important demand for a secure platform in monitoring and control Electric Vehicle Recharge systems [52].

The main issue is always centred on how cyber security deal with the cyber-attacks for industry 4.0, while mapping current topics, such as 'cloud compu-ting', 'smart grid', 'intrusion detection', 'privacy', 'internet of thing', and 'smart cities' [11], in order to keep up with this technological paradigm shift and to introduce measures that prevent significant expected fatalities [51], over disparate sectors, from e-commerce to banks, in how to cope with digitalization, keeping customers at priority [37] and in which implementation degree increases as the firm size increases, among different manufacturers [7]. In the end, the Industrial Revolution 4.0 will have eco-nomic, social, and political consequences at global level, in causing revolutionary changes in the intelligent processes of goods production and services, with likewise rising unemployment and social stratification [38];

4.5. Blockchain and cloud computing

Decentralized architectures of IoT devices have been a current debate. Last achievements on blockchain technologies, for example, allowed the use of a smart ecosystem, able to support cybersecurity mechanisms across distinct sectors such as the smart homes installations, focusing on the immutability of users and devices as well as the dynamic and immutable management of blocked malicious IPs [25]; in multiple industrial applications, healthcare, finance, and government [20] and in terms of solutions for cyber security problems such as Accountability, Traceability and Identification [12].

The point is how to better improve security of systems architecture, in order to provide protection against malicious internal users and malware implanted inside the system, which can be solved through preventive safeguards, inherent to blockchain security architecture [19]. Blockchain, may contribute to privacy, security and non-repudiation, of an IoT system, through the large amount of data generated and variety of sensors and devices adopted [2], as the blockchain technology build a scala-ble and decentralized end-to-end secure IoT system [14]. Also the IoT can be enhanced with an AI at the gateway level to detect and classify suspected activities [14]. Moreo-ver, Blockchain technology is also of use in parallel with cloud computing for higher education, in terms of primary

 doi:10.20944/preprints202110.0312.v1

infrastructure topology, putting together machine learning and artificial intelligence on training opportunities [35}

Cloud computing is therefore highly correlated with Blockchain technology in what comes to preventing attacks against, for example, radio-frequency (RF) ena-bled hardware, Internet of Things (IoT) firmware, and wireless protocols [50]. Inter-connectedness of intelligent devices and the use of public networks is at the centre of debate with regard to smart sities due to interconnected services for their citizens, in where cyber security has become a major concern [29], namely in issues such as com-munication infrastructures, cloud computing, collaborative platforms, big data, smart health and energy management [26].

The discussion on cloud computing covers subthemes of cyber security of supply chain based on software and networks, to minimize risks of purchasing and disconnection of key machines from networks [46]. To summarize, 5G and 6G networks can provide novel communication networks infrastructure, although IoT systems, will remain with the same energy capacity for hackers take advantage of this weaknesses. There is a need for a system to identify and counter potential threats in those next generation networks and decentralised systems like Blockchain [15].

5. Conclusions

The IoT has been a key element for example, for smart manufacturing, smart cit-ies, smart health, smart grids and EVs. IoT and IIoT bridges thus physical artifacts and internet, either in our daily lives or in the industry environment. In the one hand, such linkage unveils countless opportunities, while in the other hand it exposes our infor-mation and behaviors to potentially hacking sensitive data and critical infrastructure.

Additionally, IoT produces huge amounts of information that need to be protected and that is linked to varied security risks, related with its interconnectedness, either through cloud computing, or Blockchain, for example in smart factories, smart homes and smart cities. In this way, due to the need of decision making and investment, cyber security must first focus on the varying weaknesses of IoT objects and further work on its security mechanisms such as privacy, access control, data storage and authoriza-tion, whereas organizations should adopt a cyber security strategy. Therefore, organi-zations need to keep up with the development of technologies to respond appropriate-ly to cyber security threats. This study fills a gap in the IIoT cyber security and intends to encourage further research on the topic.

Furthermore, arising technologies such as Blockchain may perform a central role in the future of cyber security in IoT an IIoT, while security will become more im-portant in future because the number of object of cordless connections augment in the short term and extends to virtually all areas of our daily lives that need to be effec-tively managed.

Author Contributions: : Ricardo J. G. Raimundo and Albérico M. Rosário. All authors have read and agreed to the pub-lished version of the manu-script.For research articles with several authors, a short paragraph specifying their individual contributions must be provided. The following statements should be used “Conceptualization, X.X. and Y.Y.; methodology, X.X.; software, X.X.; validation, X.X., Y.Y. and Z.Z.; formal analysis, X.X.; investigation, X.X.; resources, X.X.; data curation, X.X.; writ-ing—original draft preparation, X.X.; writing—review and editing, X.X.; visualization, X.X.; su-pervision, X.X.; project administration, X.X.; funding acquisition, Y.Y. All authors have read and agreed to the published version of the manuscript.” Please turn to the CRediT taxonomy for the term ex-planation. Authorship must be limited to those who have contributed substantially to the work reported.

Funding: This research received no external funding.

Data Availability Statement: In this section, please provide details regarding where data supporting reported results can be found, including links to publicly archived datasets analyzed or generated during the study. Please refer to suggested Data Availability Statements in section “MDPI Research Data Policies” at https://www.mdpi.com/ethics. You might choose to exclude this statement if the study did not report any data.

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 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 2014 to 2021.

Documents		2014	2015	2016	2017	2018	2019	2020	2021	Total
An Intelligent Tree-Based Intrusion Detection Model for Cybe...	2021	-	-	-	-	-	-	-	1	**1**
User values and the development of a cybersecurity public po...	2021	-	-	-	-	-	-	1	1	**2**
A Security-UTAUT Framework for Evaluating Key Security Deter...	2021	-	-	-	-	-	-	-	1	**1**
On Australia's cyber and critical technology international e...	2020	-	-	-	-	-	-	-	1	**1**
Internet-scale Insecurity of Consumer Internet of Things	2020	-	-	-	-	-	-	1	1	**2**
A Blockchain Solution for Enhancing Cybersecurity Defence of...	2020	-	-	-	-	-	-	-	1	**1**
Scalable and Secure Architecture for Distributed IoT Systems	2020	-	-	-	-	-	-	-	1	**1**
Modeling for malicious traffic detection in 6G next generati...	2020	-	-	-	-	-	-	3	1	**4**
Awareness and readiness of Industry 4.0: The case of Turkish...	2020	-	-	-	-	-	-	1	6	**7**
Technologies, opportunities and challenges of the industrial...	2020	-	-	-	-	-	-	2	8	**10**
An overview of distributed denial of service and internet of...	2020	-	-	-	-	-	-	-	1	**1**
Artificial intelligence techniques for a scalable energy tra...	2020	-	-	-	-	-	-	-	1	**1**
20 years of scientific evolution of cyber security: A scienc...	2020	-	-	-	-	-	-	12	3	**15**
A review on the research growth of industry 4.0: IIoT busine...	2020	-	-	-	-	-	-	-	4	**4**
Toward a cloud computing learning community	2019	-	-	-	-	-	-	1	2	**3**
Towards the integration of a post-hoc interpretation step in...	2019	-	-	-	-	-	-	-	2	**2**
Proactive antifragility: A new paradigm for next-generation ...	2019	-	-	-	-	-	-	-	1	**1**
A Research on the Vulnerabilities of PLC using Search Engine	2019	-	-	-	-	-	-	1	-	**1**
Cyber security threat intelligence using data mining techniq...	2019	-	-	-	-	-	-	2	1	**3**
Addressing Industry 4.0 Cybersecurity Challenges	2019	-	-	-	-	-	1	9	12	**22**

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 October 2021 doi:10.20944/preprints202110.0312.v1

FACTS approach to address cybersecurity issues in electric v...	2019	-	-	-	-	-	4	3	3	**10**
Towards Industry 4.0: Mapping digital technologies for suppl...	2019	-	-	-	-	-	12	50	47	**111**
Evaluating security of low-power internet of things networks	2019	-	-	-	-	-	1	7	-	**8**
Legitimate firms or hackers - who is winning the global cybe...	2019	-	-	-	-	-	-	2	1	**3**
Foresight of cyber security threat drivers and affecting tec...	2018	-	-	-	-	-	1	3	5	**9**
Agile Business Growth and Cyber Risk:	2018	-	-	-	-	-	1	1	-	**2**
How to compete in the age of artificial intelligence: Implem...	2018	-	-	-	-	-	1	1	2	**4**
Solving Global Cybersecurity Problems by Connecting Trust Us...	2018	-	-	-	-	-	1	-	1	**2**
A Cybersecurity Case for the Adoption of Blockchain in the F...	2018	-	-	-	-	-	-	1	1	**2**
Cybersecurity Attacks and Defences for Unmanned Smart Ships	2018	-	-	-	-	-	-	5	1	**6**
Avoiding the internet of insecure industrial things	2018	-	-	-	-	5	14	8	9	**36**
The impact of China's 2016 Cyber Security Law on foreign tec...	2018	-	-	-	-	6	3	6	5	**20**
Adoption of industry 4.0 technologies in supply chains	2018	-	-	-	-	-	1	3	2	**6**
Artificial intelligence in smart tourism: A conceptual frame...	2018	-	-	-	-	-	1	2	5	**8**
Cybersecurity and the auto industry: The growing challenges ...	2018	-	-	-	-	-	3	5	1	**9**
Information innovation technology in smart cities	2017	-	-	-	-	-	3	-	-	**3**
Kill switches, remote deletion, and intelligent agents:	2017	-	-	-	-	2	-	2	3	**7**
Blockchain technology innovations	2017	-	-	-	-	11	46	60	37	**155**
Personality traits and cyber-attack victimisation: Multiple ...	2017	-	-	-	-	-	-	4	-	**4**
STM32-based vehicle data acquisition system for Internet-of-...	2017	-	-	-	1	2	4	5	5	**17**
Electronic finance – recent developments	2017	-	-	-	2	1	-	6	3	**12**
Cybersecurity in the Internet of Things: Legal aspects	2016	-	-	-	4	16	14	10	7	**51**
	Total	**-**	**-**	**-**	**7**	**43**	**111**	**217**	**187**	**568**

Appendix B

Table A2. Overview of document self-citation period 2014 to 2021.

Documents	2014	2015	2016	2017	2018	2019	2020	2021	Total

A Security-UTAUT Framework for Evaluating Key Security Deter...	2021	-	-	-	-	-	-	-	1	**1**
On Australia's cyber and critical technology international e...	2020	-	-	-	-	-	-	-	1	**1**
Internet-scale Insecurity of Consumer Internet of Things	2020	-	-	-	-	-	-	1	-	**1**
Modeling for malicious traffic detection in 6G next generati...	2020	-	-	-	-	-	-	2	-	**2**
Technologies, opportunities and challenges of the industrial...	2020	-	-	-	-	-	-	-	1	**1**
20 years of scientific evolution of cyber security: A scienc...	2020	-	-	-	-	-	-	10	-	**10**
Toward a cloud computing learning community	2019	-	-	-	-	-	-	-	1	**1**
Towards the integration of a post-hoc interpretation step in...	2019	-	-	-	-	-	-	-	1	**1**
Addressing Industry 4.0 Cybersecurity Challenges	2019	-	-	-	-	-	-	-	1	**1**
Emerging technologies and risk: How do we optimize enterpris...	2019	-	-	-	-	-	4	3	1	**8**
FACTS approach to address cybersecurity issues in electric v...	2019	-	-	-	-	-	1	-	1	**2**
Towards Industry 4.0: Mapping digital technologies for suppl...	2019	-	-	-	-	-	-	5	-	**5**
Legitimate firms or hackers - who is winning the global cybe...	2019	-	-	-	-	-	-	1	1	**2**
Solving Global Cybersecurity Problems by Connecting Trust Us...	2018	-	-	-	-	-	-	-	1	**1**
Avoiding the internet of insecure industrial things	2018	-	-	-	-	-	2	-	-	**2**
Adoption of industry 4.0 technologies in supply chains	2018	-	-	-	-	-	1	-	-	**1**
Cybersecurity and the auto industry: The growing challenges ...	2018	-	-	-	-	-	-	1	-	**1**
Blockchain technology innovations	2017	-	-	-	-	1	1	-	1	**3**
Electronic finance – recent developments	2017	-	-	-	-	-	-	2	-	**2**
Cybersecurity in the Internet of Things: Legal aspects	2016	-	-	-	1	-	1	-	-	**2**
	Total	**-**	**-**	**-**	**1**	**1**	**10**	**25**	**11**	**48**

References

1. Alshboul, Y., Bsoul, A. A. R., AL Zamil, M., & Samarah, S. (2021). Cybersecurity of smart home systems: Sensor identity protection. Journal of Network and Systems Management, 29(3) doi:10.1007/s10922-021-09586-9
2. Occa, R., Borbon-Galvez, Y., & Strozzi, F. (2020). In search of lost security. A systematic literature review on how blockchain can save the iot revolution. Paper presented at the Proceedings of the Summer School Francesco Turco,
3. Khalid, A., Sundararajan, A., Hernandez, A., & Sarwat, A. I. (2019). FACTS approach to address cybersecurity issues in electric vehicle battery systems. Paper presented at the 2019 IEEE Technology and Engineering Management Conference, TEMSCON 2019, doi:10.1109/TEMSCON.2019.8813669

4. Xie, Y., Su, X., He, Y., Chen, X., Cai, G., Xu, B., & Ye, W. (2017). STM32-based vehicle data acquisition system for internet-of-vehicles. Paper presented at the Proceedings - 16th IEEE/ACIS International Conference on Computer and Information Science, ICIS 2017, 895-898. doi:10.1109/ICIS.2017.7960119
5. Mangino, A., Pour, M. S., & Bou-Harb, E. (2020). Internet-scale insecurity of consumer internet of things. ACM Transactions on Management Information Systems, 11(4) doi:10.1145/3394504
6. Lee, T., Kim, S., & Kim, K. (2019). 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, 184-188. doi:10.1109/ICTC46691.2019.8939961
7. Sarı, T., Güleş, H. K., & Yiğitol, B. (2020). Awareness and readiness of industry 4.0: The case of turkish manufacturing industry. Advances in Production Engineering and Management, 15(1), 57-68. doi:10.14743/APEM2020.1.349
8. Gupta, S., Sabitha, A. S., & Punhani, R. (2019). Cyber security threat intelligence using data mining techniques and artificial intelligence. International Journal of Recent Technology and Engineering, 8(3), 6133-6140. doi:10.35940/ijrte.C5675.098319
9. Uzunov, A. V., Nepal, S., & Baruwal Chhetri, M. (2019). Proactive antifragility: A new paradigm for next-generation cyber defence at the edge. Paper presented at the Proceedings - 2019 IEEE 5th International Conference on Collaboration and Internet Computing, CIC 2019, 246-255. doi:10.1109/CIC48465.2019.00039
10. Smith, K. J., Dhillon, G., & Carter, L. (2021). User values and the development of a cybersecurity public policy for the IoT. International Journal of Information Management, 56 doi:10.1016/j.ijinfomgt.2020.102123
11. Furstenau, L. B., Sott, M. K., Homrich, A. J. O., Kipper, L. M., Al Abri, A. A., Cardoso, T. F., . . . Cobo, M. J. (2020). 20 years of scientific evolution of cyber security: A science mapping. Paper presented at the Proceedings of the International Conference on Industrial Engineering and Operations Management, , 0(March) 314-325.
12. Gorog, C., & Boult, T. E. (2018). Solving global cybersecurity problems by connecting trust using blockchain. Paper presented at the Proceedings - IEEE 2018 International Congress on Cybermatics: 2018 IEEE Conferences on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, iThings/GreenCom/CPSCom/SmartData/Blockchain/CIT 2018, 1425-1432. doi:10.1109/Cybermatics_2018.2018.00243
13. Urquhart, L., & McAuley, D. (2018). Avoiding the internet of insecure industrial things. Computer Law and Security Review, 34(3), 450-466. doi:10.1016/j.clsr.2017.12.004
14. Dhieb, N., Ghazzai, H., Besbes, H., & Massoud, Y. (2020). Scalable and secure architecture for distributed IoT systems. Paper presented at the 2020 IEEE Technology and Engineering Management Conference, TEMSCON 2020, doi:10.1109/TEMSCON47658.2020.9140108
15. Ghorbani, H., Mohammadzadeh, M. S., & Ahmadzadegan, M. H. (2020). Modeling for malicious traffic detection in 6G next generation networks. Paper presented at the 2020 International Conference on Technology and Entrepreneurship - Virtual, ICTE-V 2020, , 2020-April doi:10.1109/ICTE-V50708.2020.9113777
16. Raban, Y., & Hauptman, A. (2018). Foresight of cyber security threat drivers and affecting technologies. Foresight, 20(4), 353-363. doi:10.1108/FS-02-2018-0020
17. Vaccari, I., Cambiaso, E., & Aiello, M. (2019). Evaluating security of low-power internet of things networks. International Journal of Computing and Digital Systems, 8(2), 101-114. doi:10.12785/ijcds/080202
18. Laskurain-Iturbe, I., Arana-Landín, G., Landeta-Manzano, B., & Uriarte-Gallastegi, N. (2021). Exploring the influence of industry 4.0 technologies on the circular economy. Journal of Cleaner Production, 321 doi:10.1016/j.jclepro.2021.128944
19. Kis, M., & Singh, B. (2018). A cybersecurity case for the adoption of blockchain in the financial industry. Paper presented at the Proceedings - IEEE 2018 International Congress on Cybermatics: 2018 IEEE Conferences on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, iThings/GreenCom/CPSCom/SmartData/Blockchain/CIT 2018, 1491-1498. doi:10.1109/Cybermatics_2018.2018.00252
20. Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J., & Amaba, B. (2017). Blockchain technology innovations. Paper presented at the 2017 IEEE Technology and Engineering Management Society Conference, TEMSCON 2017, 137-141. doi:10.1109/TEMSCON.2017.7998367
21. Parasol, M. (2018). The impact of china's 2016 cyber security law on foreign technology firms, and on china's big data and smart city dreams. Computer Law and Security Review, 34(1), 67-98. doi:10.1016/j.clsr.2017.05.022
22. Khatkar, M., Kumar, K., & Kumar, B. (2020). An overview of distributed denial of service and internet of things in healthcare devices. Paper presented at the Proceedings of International Conference on Research, Innovation, Knowledge Management and Technology Application for Business Sustainability, INBUSH 2020, 44-48. doi:10.1109/INBUSH46973.2020.9392171
23. Al-Omari, M., Rawashdeh, M., Qutaishat, F., Alshira'H, M., & Ababneh, N. (2021). An intelligent tree-based intrusion detection model for cyber security. Journal of Network and Systems Management, 29(2) doi:10.1007/s10922-021-09591-y
24. Nomm, S., Guerra-Manzanares, A., & Bahsi, H. (2019). Towards the integration of a post-hoc interpretation step into the machine learning workflow for IoT botnet detection. Paper presented at the Proceedings - 18th IEEE International Conference on Machine Learning and Applications, ICMLA 2019, 1162-1169. doi:10.1109/ICMLA.2019.00193
25. Giannoutakis, K. M., Spathoulas, G., Filelis-Papadopoulos, C. K., Collen, A., Anagnostopoulos, M., Votis, K., & Nijdam, N. A. (2020). A blockchain solution for enhancing cybersecurity defence of IoT. Paper presented at the Proceedings - 2020 IEEE International Conference on Blockchain, Blockchain 2020, 490-495. doi:10.1109/Blockchain50366.2020.00071

26. Ismail, L., & Zhang, L. (2017). Information innovation technology in smart cities. Information innovation technology in smart cities (pp. 1-356) doi:10.1007/978-981-10-1741-4
27. Dandapani, K. (2017). Electronic finance – recent developments. Managerial Finance, 43(5), 614-626. doi:10.1108/MF-02-2017-0028
28. Morris, D., Madzudzo, G., & Garcia-Perez, A. (2018). Cybersecurity and the auto industry: The growing challenges presented by connected cars. International Journal of Automotive Technology and Management, 18(2), 105-118. doi:10.1504/IJATM.2018.092187
29. Grandhi, L. S., Grandhi, S., & Wibowo, S. (2021). 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, 17-22. doi:10.1109/SNPDWinter52325.2021.00013
30. Dalmarco, G., & Barros, A. C. (2018). Adoption of industry 4.0 technologies in supply chains doi:10.1007/978-3-319-74304-2_14
31. Rafaqat, M., Ishfaq, K., & Ahmed, N. (2019). Implementation of augmented reality in the context of industry 4.0: A comprehensive review. Paper presented at the Proceedings of the International Conference on Industrial Engineering and Operations Management, 93-94.
32. Ardito, L., Petruzzelli, A. M., Panniello, U., & Garavelli, A. C. (2019). Towards industry 4.0: Mapping digital technologies for supply chain management-marketing integration. Business Process Management Journal, 25(2), 323-346. doi:10.1108/BPMJ-04-2017-0088
33. Chaykin, A. (2019). New systems, new cyber threats. Petroleum Economist, 86(9), 32-33.
34. Culot, G., Fattori, F., Podrecca, M., & Sartor, M. (2019). Addressing industry 4.0 , cybersecurity challenges. IEEE Engineering Management Review, 47(3), 79-86. doi:10.1109/EMR.2019.2927559
35. Foster, D., White, L., Erdil, D. C., Adams, J., Argüelles, A., Hainey, B., . . . Stott, L. (2019). Toward a cloud computing learning community. Paper presented at the Annual Conference on Innovation and Technology in Computer Science Education, ITiCSE, 143-155. doi:10.1145/3344429.3372506
36. Mohanty, S., & Vyas, S. (2018). How to compete in the age of artificial intelligence: Implementing a collaborative human-machine strategy for your business. How to compete in the age of artificial intelligence: Implementing a collaborative human-machine strategy for your business (pp. 1-229) doi:10.1007/978-1-4842-3808-0
37. Gupta, R. (2021). Industry 4.0 adaption in indian banking Sector—A review and agenda for future research. Vision, doi:10.1177/09722629211996829
38. Rymarczyk, J. (2020). Technologies, opportunities and challenges of the industrial revolution 4.0: Theoretical considerations. Entrepreneurial Business and Economics Review, 8(1), 185-198. doi:10.15678/EBER.2020.080110
39. Dube, D. P., & Mohanty, R. P. (2020). Towards development of a cyber security capability maturity model. International Journal of Business Information Systems, 34(1), 104-127. doi:10.1504/IJBIS.2020.106800
40. Albladi, S. M., & George, R. S. (2017). Personality traits and cyber-attack victimisation: Multiple mediation analysis. Paper presented at the Joint 13th CTTE and 10th CMI Conference on Internet of Things - Business Models, Users, and Networks, , 2018-January 1-6. doi:10.1109/CTTE.2017.8260932
41. Sivakumar, S., Siddappa Naidu, K., & Karunanithi, K. (2019). Design of energy management system using autonomous hybrid micro-grid under IOT environment. International Journal of Recent Technology and Engineering, 8(2 Special Issue 2), 338-343. doi:10.35940/ijrte.B1058.0782S219
42. Gary, R. F., Marinakis, Y., Majadillas, M. A., White, R., & Walsh, S. T. (2019). Legitimate firms or hackers - who is winning the global cyber war? International Journal of Technology Intelligence and Planning, 12(3), 297-314. doi:10.1504/IJTIP.2019.099243
43. Griffy-Brown, C., Miller, H., Zhao, V., Lazarikos, D., & Chun, M. (2019). Emerging technologies and risk: How do we optimize enterprise risk when deploying emerging technologies? Paper presented at the 2019 IEEE Technology and Engineering Management Conference, TEMSCON 2019, doi:10.1109/TEMSCON.2019.8813743
44. Murshida, Faizabadi, A. R., Basthikodi, M., & Akram, K. (2019). Trust management in internet of things applications. International Journal of Recent Technology and Engineering, 8(2 Special Issue 8), 1750-1753. doi:10.35940/ijrte.B1146.0882S819
45. Hitefield, S. D., Fowler, M., & Clancy, T. C. (2018). Exploiting buffer overflow vulnerabilities in software defined radios. Paper presented at the Proceedings - IEEE 2018 International Congress on Cybermatics: 2018 IEEE Conferences on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, iThings/GreenCom/CPSCom/SmartData/Blockchain/CIT 2018, 1921-1927. doi:10.1109/Cybermatics_2018.2018.00318
46. Latif, M. N. A., Aziz, N. A. A., Hussin, N. S. N., & Aziz, Z. A. (2021). Cyber security in supply chain management: A systematic review. [Bezpieczeństwo cybernetyczne w zarządzaniu łańcuchem dostaw] Logforum, 17(1), 49-57. doi:10.17270/J.LOG.2021555
47. Soldani, D. (2021). 6g fundamentals: Vision and enabling technologies. Journal of Telecommunications and the Digital Economy, 9(3), 58-86. doi:10.18080/JTDE.V9N3.418
48. Weber, R. H., & Studer, E. (2016). Cybersecurity in the internet of things: Legal aspects. Computer Law and Security Review, 32(5), 715-728. doi:10.1016/j.clsr.2016.07.002

49. Sayed-Mouchaweh, M. (2020). Artificial intelligence techniques for a scalable energy transition: Advanced methods, digital technologies, decision support tools, and applications. Artificial intelligence techniques for a scalable energy transition: Advanced methods, digital technologies, decision support tools, and applications (pp. 1-382) doi:10.1007/978-3-030-42726-9
50. Oconnor, T. J., & Stricklan, C. (2021). Teaching a hands-on mobile and wireless cybersecurity course. Paper presented at the Annual Conference on Innovation and Technology in Computer Science Education, ITiCSE, 296-302. doi:10.1145/3430665.3456346
51. Memon, K. R., & Ooi, S. K. (2021). THE DARK SIDE OF INDUSTRIAL REVOLUTION 4.0-IMPLICATIONS AND SUGGESTIONS. Academy of Entrepreneurship Journal, 27(SpecialIssue 2), 1-18.
52. Terruggia, R., & Garrone, F. (2020). Secure IoT and cloud based infrastructure for the monitoring of power consumption and asset control. Paper presented at the 12th AEIT International Annual Conference, AEIT 2020, doi:10.23919/AEIT50178.2020.9241195
53. Sahu, A. K., Sahu, A. K., & Sahu, N. K. (2020). A review on the research growth of industry 4.0: IIoT business architectures benchmarking. International Journal of Business Analytics, 7(1), 77-97. doi:10.4018/IJBAN.2020010105
54. Nash, I. (2021). Cybersecurity in a post-data environment: Considerations on the regulation of code and the role of producer and consumer liability in smart devices. Computer Law and Security Review, 40 doi:10.1016/j.clsr.2021.105529
55. Silverajan, B., Ocak, M., & Nagel, B. (2018). Cybersecurity attacks and defences for unmanned smart ships. Paper presented at the Proceedings - IEEE 2018 International Congress on Cybermatics: 2018 IEEE Conferences on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, iThings/GreenCom/CPSCom/SmartData/Blockchain/CIT 2018, 15-20. doi:10.1109/Cybermatics_2018.2018.00037
56. Rosário, A., and Raimundo, R. (2021). Importance of Value Propositions in Marketing: Research and Challenges, Academy of Strategic Management Journal, 20(2), 1-23. doi.org/1939-6104-20-S2-163
57. Raimundo, R. and Rosário, A., (2021). Blockchain system in the Higher Education, European Journal of Investigation in Health, Psychology and Education, 11(1), 276-293. doi.org/10.3390/ejihpe1101002
58. Rosário. A., Vilaça, F., Raimundo, R., and Cruz, R. (2021). Literature review on Health Knowledge Management in the last 10 years (2009-2019), The Electronic Journal of Knowledge Management, 18(3), 338-355. doi.org/10.34190/ejkm.18.3.2120
59. Soldani, D. (2020). On australia's cyber and critical technology international engagement strategy towards 6G how australia may become a leader in cyberspace. Journal of Telecommunications and the Digital Economy, 8(4), 127-158. doi:10.18080/JTDE.V8N4.340
60. Oravec, J. A. (2017). Kill switches, remote deletion, and intelligent agents: Framing everyday household cybersecurity in the internet of things. Technology in Society, 51, 189-198. doi:10.1016/j.techsoc.2017.09.004
61. Griffy-Brown, C., Lazarikos, D., & Chun, M. (2018). Agile business growth and cyber risk: Paper presented at the 2018 IEEE Technology and Engineering Management Conference, TEMSCON 2018, doi:10.1109/TEMSCON.2018.8488397
62. Čapek, J. (2018). Cybersecurity and internet of things. Paper presented at the IDIMT 2018: Strategic Modeling in Management, Economy and Society - 26th Interdisciplinary Information Management Talks, 343-349.
63. Tsaih, R. -., & Hsu, C. C. (2018). Artificial intelligence in smart tourism: A conceptual framework. Paper presented at the Proceedings of the International Conference on Electronic Business (ICEB), , 2018-December 124-133..