Cybersecurity in Industrial Management within the Internet of Things

Sachin Vasant Dorage[1]

[1] Sachin Vasant Dorage Lead System Administrator Information Technology Oriental College of Pharmacy, Navi Mumbai, Maharashtra, India

---***---

Abstract - Recently, it has become important to integrate cybersecurity threat management policies in the management of any organization that uses information systems, whether large, medium or even small organizations. People live in the center of the field of smart homes, business opportunities of smart industrial cities and healthcare. Even as IoT security issues become increasingly ubiquitous in the industrial realm, they face the added challenge of evolving networks. Architecture towards the integration of information technology (IT) and operational technology (OT) networks. This article analyzes the underlying cybersecurity risks, attack landscape in the Industrial IoT (IIoT), and suggests possible countermeasures for future hybrid IoT applications, based on lessons learned from IIoT projects. Security is essential for IoT systems to protect sensitive data and infrastructure, while security issues are becoming increasingly costly, especially in the industrial sector. The domains of the Internet of Things (IIoT). With this in mind, the issue of cybersecurity has become paramount for the Internet of Things (IoT) and the Industrial Internet of Things (IIoT) to mitigate cybersecurity risks for organizations and end users. New cybersecurity technologies and applications have improved IoT security management. However, there is a disparity in the effectiveness of solutions for IoT cyber risks.

***Key Words*:** Cybersecurity; Computer security; IT security; Internet of things (IoT); Safety; Industrial internet of things (IIoT); Blockchain and SDN (Software Defined Networking); 5G

1. INTRODUCTION

The Internet of Things (IoT) seeks to integrate the physical and digital worlds into a unified system, opening up substantial business prospects for various industries, including healthcare and energy. Despite these opportunities, IoT faces numerous security challenges that are often more intricate than those in other domains due to its intricate environment and the vast array of devices, which are resource-limited (Kouicem, 2018). The Internet of Things (IoT) refers to the interconnected network of physical devices, vehicles, and home appliances (Biljana L. Risteska Stojkoska, 2017)and other gadgets and devices (mechatronic systems) with embedded electronics, software, sensors, actuators, and connectivity, which enables them to connect, collect and exchange data (htt) (Figure 1). A critical utility for IoT is a? Clever factory? (Figure 2) (Muhammad Shoaib Farooq) In a smart factory, there are four key components to consider people, processes, technological ecosystem, and intelligent objects. It is projected that by 2025, Internet of Things (IoT) applications will produce 1.2 to 3.7 trillion USD in annual economic value in these smart factories (Arbia Riahi Sfar a b, 2017). The intelligent industry has embarked on a highly beneficial initiative by incorporating IoT technology within the industrial sector. As predicted, superior technology and enterprise ought to clear up several troubles with the aid of using imposing pervasive security countermeasures through the effective implementation of the IoT (Lin, et al., 2017). The today's implementation of the IoT is fixing business safety issues by providing productive and cost-effective solutions (Salman, Zolanvari, Erbad, Jain, & Samaka, 2018). The Internet of Things (IoT) has thus gained widespread adoption across various industries, including the Internet of Battlefield Things (IoBT) and the Internet of Vehicles (IoV) (Khalid, 2019), (Uzunov, Nepal, & Chhetri, 2019), In addition to its security challenges, there has been a rise in cyber-attacks. As a result, there is growing apprehension regarding cybersecurity in this area, compounded by insufficient policy guidance and a limited comprehension of user values associated with cybersecurity in the context of the Internet of Things (IoT). Furthermore, policy development has not been informed by the values of key stakeholders (Smith, 2021). Cybersecurity focuses on safeguarding electronic devices, software applications, and data, as well as the methods used to access these systems. The primary security goals typically include ensuring privacy, which involves preventing unauthorized entities from accessing, altering, or destroying sensitive information (Michele Kremer Sott*, 2020),As a result of the numerous IoT (Gorog Christopher, 2018) connected devices in existence, society is facing a growing risk of cyber-attacks like denial-of-service attacks (Lachlan Urquhart, 2018)preventing direct access to devices, for example, by hackers and insiders (Najmeddine Dhieb, 2020). Technology plays an ever-growing role in our everyday lives, leading to the continuous advancement of cybercrime and cybersecurity measures (Yoel Raban, 2018), (Ivan Vaccari, 2019), throughout the entire manufacturing industry (Iker Laskurain-Iturbe, 2021), there is a necessity to invest in cybersecurity measures as new technologies are being developed for managing IoT cybersecurity (Kis & Singh, 2018), Additionally, smart grids are highly susceptible to cyber-attacks, which can result in significant costs and severe impacts on the safety of citizens and governments (Lachlan Urquhart, 2018). There is a rising apprehension regarding cybersecurity and the absence of efficient safeguards, for instance, cybersecurity professionals (T. Ahram, 2017). As an example, China is formulating a new cybersecurity law and strategy (Parasol, 2018). Additionally, with healthcare being a prominent issue due to the vast amount of crucial data involved, cybersecurity measures tend to be lacking in hospitals, putting patients' lives and trust in jeopardy (Khatkar Monika, 2020). The existing literature primarily examines the technical aspects of IoT cybersecurity, leaving a void in terms of frameworks to tackle the intricate cybersecurity challenges within the IoT ecosystem. This study conducts a thorough literature review on IoT security technologies and cyber risk management within the Here's how the article is structured: Section 2 covers various theoretical concepts concerning cybersecurity in the IoT. Section 3 outlines the methodological approach employed in this study. Moving on to Section 4, we delve into the primary applications of cybersecurity in relation to the Internet of Things, as identified in existing literature. To wrap up, we offer insights into potential implications and directions for future research industry.

2. Literature Review: Key Concepts

It is essential to have a clear understanding of the concepts discussed before delving into the latest trends in cyber-attacks and IoT systems.

2.1. Cybersecurity

Cybersecurity is now a significant issue because numerous everyday items can be linked to the Internet, a crucial aspect of our daily routines. If it can be linked, it can be breached. Therefore, the focus of cybersecurity is on intrusion detection (Mohammad Al-Omari, 2021), where physical or cloud computing operations are supervised by examining system weaknesses and behavioral trends (Alejandro Guerra-Manzanares, 2019). Cyber threats can manifest as distributed denial of service (DDoS) attacks (Lachlan Urquhart, 2018), malicious IPs (K. M. Giannoutakis, 2020), and data tampering, leading to consequences like data loss, financial setbacks, and potential harm to health (Khatkar Monika, 2020).

2.2. The Internet of Things

As mentioned earlier, the Internet of Things (IoT) is a concept that combines the existing internet with physical objects (Alshboul, Bsoul, Zamil, & Samarah, 2021).

With this in mind, the IoT significantly increases the many connected devices and devices in our lives, for example, in smart grids (Furstenau, et al., 2020) and in transportation through electric vehicles (EVs) (Khalid, 2019). Thus, Internet technology, although it presents countless advantages, also presents serious threats (Morris, Madzudzo, & Garcia-Perez, 2018). Therefore, IoT applications cover a wide range of objects, from smart homes (K. M. Giannoutakis, 2020) to large smart factories (Lee, Kim, & Kim, 2019)to smart networks (Lachlan Urquhart, 2018). However, the relevant devices are complemented by wireless interfaces of wireless sensor networks (WSNs) that constitute a key IoT technology (Alshboul, Bsoul, Zamil, & Samarah, 2021), (Occa, Borbon-Galvez, & Strozzi, 2020) for the wide flow of IoT systems. Examples include "Smart Grid", "Internet of Things", "Manufacturing Systems", "Smart Cities" and "Cloud Computing in Transportation and Smart Homes" (Lee, Kim, & Kim, 2019), (Gupta, Sabitha, & Punhani, 2019), (Furstenau, et al., 20 years of scientific evolution of cyber security, 2020), (K. M. Giannoutakis, 2020). On the one hand, in the case of smart homes, it is advisable to protect the identity of the sensors from recognition through the networks of the wireless communication environment, keeping the software updated with reliable providers and cloud providers (Alshboul, Bsoul, Zamil, & Samarah, 2021). On the opposite hand, with inside the case of clever cities, to which many populations will generally tend to migrate, the IoT offers numerous services such as smart parking, environment, waste, water and traffic management, or even the energy consumption monitoring, through operations that include the IoT spectrum, its energy and architectural efficiency, and the mitigation of its environmental effects, keeping in mind its contextual interaction Rephrase (Ismail & Zhang, 2017), (Grandhi, Grandhi, & Wibowo, 2021).

2.3 The Industrial Internet of Things (IIoT)

The Riot provides numerous nuances that differentiate it from the conventional IoT. While the IoT operates in home environs, the Riot operates in business environs. In this way, it includes the optimization of deliver chains, for instance. The Riot equals Industry 4.0 (Albladi & George, 2017), that is a shared time for technology and theories of cost chain organization (Iker Laskurain-Iturbe, 2021), (Rafaqat, Ishfaq, & Ahmed, 2019). Industry 4.0 affords a modular structure, through which computer systems reveal and control clever factories and resulting physical techniques (Ardito, Petruzzelli, Panniello, & Garavelli, 2018), developing a virtual reproduction of the bodily techniques at the same time as making decentralized decisions (Chaykin, 2019). Along the way, pc structures engage each with each other and with people (Dalmarco & Barros, 2018). In addition, each organizational and interorganizational offerings may be furnished to actors of the delivery chain. Interconnected objects, controlled and accessed through information mining strategies along with Blockchain, can be partially accessed and characteristic as sensors and are enabled to engage with different device (Culot, Fattori, Podrecca, & Sartor, 2019), (Foster, et al., 2019). Such systems, made from clever artifacts inside the IoT system, call for minimum or no Human movement so that you can trade and bring data, frequently assisted via way of means of synthetic intelligence mechanisms (Mohanty & Vyas, 2018). In summary, the Riot? s primary worries encompass decreasing fabric and strength consumption, higher handling the temporal dimensions Of safety in phrases of ?intrusion detection?, cloud computing, and the interface among deliver chain control and marketing Processes, plus higher handling the complexity of infrastructures in phrases of the variety of access points (Furstenau, et al., 20 years of scientific evolution of cyber security, 2020), (Iker Laskurain-Iturbe, 2021), (Ardito, Petruzzelli, Panniello, & Garavelli, 2018), (Culot, Fattori, Podrecca, & Sartor, 2019), (Gupta R. , 2021), (Rymarczyk, 2020). The Riot contains each cybersecurity and IoT worries in general. It makes a specialty of integrity, wherein statistics is covered from amendment via way of means of unauthorized parties; authentication, wherein the statistics supply is proven because the pretended identity (Dube & Mohanty, 2020); privacy, wherein users? identities are non-traceable from their behaviors; (Albladi & George, 2017) confidentiality, in Which statistics is made unintelligible to unauthorized entities; and availability, wherein the machine offerings are to be had most effective for valid therefore faces essential challenges, specifically concerning operations in decentralized environs including Blockchain systems (Gary, Marinakis, Majadillas, White, & Walsh, 2019), (Griffy-Brown, Miller, Zhao, Lazarikos, & Chun, 2019) and the various nature of clever artifacts (Murshida, Faizabadi, Basthikodi, & Akram, 2019). In addition, it is far really well worth bringing up the sparse computational assets and power to be hard to the numerous sensors that bring about inadequate conventional protection measures (Uzunov, Nepal, & Chhetri, 2019), (Hitefield, Fowler, & Clancy, 2019). The aforementioned issues increase the chances of cyber-attacks on IoT systems, namely plants, transport, and household appliances (Uzunov, Nepal, & Chhetri, 2019), demanding substantial improvement In phrases of authentication from far off systems, encryption from new sensors, and net interface and pc software program for intrusion detection (Latif, et al., 2015). Additionally, the greater IoT innovation, the greater advanced Wi-Fi technology are, as with inside the case of 5G, that's optimized properly past voice and data, imparting a sizeable array of opportunities (Ghorbani, Mohammadzadeh, & Ahmadzadegan, 2020), (Soldani, 2021). The literature assessment provided right here additionally shows a of safety answers for cordless sensor networks with recognize to the IoT (Weber & Studer, 2016), (Oconnor & Stricklan, 2021). In particular, in phrases of net-paintings computing, decentralized architectures made from limitless objects (Ghorbani, Mohammadzadeh, & Ahmadzadegan, 2020) which include Blockchain (K. M. Giannoutakis, 2020) and cloud computing structures ease community control and configuration (Memon & Ooi, 2021), (Terruggia & Garrone, 2020), ameliorating IoT security (Sahu, Sahu, & Sahu, 2020)via sensors that optimize information sending, heading off the redundancy with inside the Wi-Fi channels through structures that enhance networking along with massive information (Iker Laskurain-Iturbe, 2021), (Dalmarco & Barros, 2018), (Nash, 2021), (Silverajan, Ocak, & Nagel, 2018).

The layout of the conceptual and technological framework for this text became now no longer made randomly; however as an alternative through an initial search On Scopus with the keywords? Internet of Things? and? Cybersecurity? , with the effects proven and mentioned with inside the following sections.

3. Materials and Methods

This study employs a Systematic Review of Biometric Literature (LRSB), as outlined by Rosario and Raymundo, Raymundo and Rosario, and Rosario et al. This qualitative methodology focuses on the analysis and synthesis of documents related to cybersecurity within the Internet of Things in Industrial Management, thereby providing various contexts for the rationale behind the studies through a rigorous and precise design. It consolidates relevant research, thereby enhancing practical knowledge for decision-making processes. A key benefit of qualitative research lies in its capacity to gather and analyze data concerning cybersecurity elements in the Internet of Things within Industrial Management. The LRSB framework is structured and transparent, offering guidance for the development of frameworks, proposing innovative approaches for future research, and identifying the research methods employed. This methodology aims to generate new insights into the cybersecurity landscape of the Internet of Things in Industrial Management. The LRSB approach is categorized into three levels and six stages, as proposed by Rosario and Raymundo, Raymundo and Rosario, and Rosario et al. in 2021.

Table 1. The systematic LRSB process (Rosário, 2022).

Phase	**Step**	**Description**
Exploration	Step 1	Problem of research
	Step 2	Exploration of suitable literature.
	Step 3	The essential accuracy of the selected research studies.
	Step 4	Integration of information from various sources.
Communication of Interpretation	Step 5	reports and recommendations
	Step 6	presentation of the LRSB report

The indexing database utilized for scientific and academic documents was Scopus, which is recognized as a leading peer-reviewed resource within the scientific and academic community. This database encompasses nearly 19,500 titles from over 5,000 international publishers, including 16,500 peer-reviewed journals across various scientific and academic disciplines. It is important to note that this study is limited by its exclusive reliance on the Scopus indexing database, thereby omitting other scientific and academic indexing resources. The bibliographic research encompasses peer-reviewed scientific and academic documents published up to September 2021. The initial search employed the keywords "Cyber Security" and "Internet of Things" to identify relevant summaries, titles, and keywords. Initially, 15,748 documents were found using the keyword "Cyber Security," which was subsequently narrowed down to 1,316 by incorporating the keyword "Internet of Things." The scope of the research was further refined to the domain of "Business, Management, and Accounting" to focus on the most pertinent studies (Table 2).

Table 2. The methodology for screening bibliographic research (Rosário, 2022).

Database Scopus	**Screening**	**Publications**
Meta-search	keyword: Cyber Security	15,748
First Inclusion Criterion	keyword: Cyber Security, Internet of Things	1316
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	

Content techniques and thematic analysis were employed to identify, examine, and report on the various documents presented by Rosário and Raimundo (2021), Raimundo and Rosário (2021), and Rosário et al. (2021). The subsequent analysis of the 60 scientific and/or academic documents indexed in Scopus will be conducted through narrative and bibliometric methods to explore the content and potential emergence of common themes that directly address the research question (Rosário and Raimundo, 2021; Raimundo and Rosário, 2021; Rosário et al., 2021). Among the selected documents, 28 were conference papers, 24 were articles, 4 were reviews, 3 were books, and 1 was a book chapter and short survey.

In terms of publication distribution, the peak number of peer-reviewed articles on the topic during the period from 2014 to 2021 occurred in 2019, with a total of 15 publications. **Figure 1** illustrates the published peer-reviewed literature for the 2014–2021 timeframe. The publications were categorized as follows: four documents were published in Computer Law and Security Review and Proceedings of the IEEE 2018 International Congress on Cybermatics; three documents appeared in the International Journal of Recent Technology and Engineering; and two documents were featured in the 2019 IEEE Technology and Engineering Management Conference, among others. The interest in this subject has fluctuated over time.

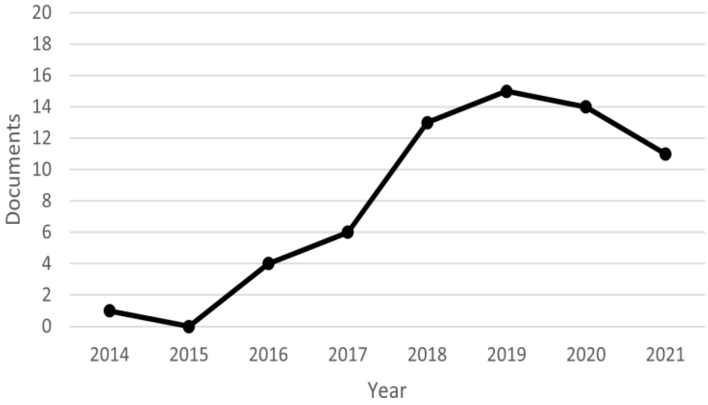

Figure 1. The number of documents per year (Rosário, 2022).

Table 3 presents an analysis of the Scimago Journal and Country Rank (SJR), highlighting the top quartile and the H index based on publication metrics.

Table 3. Impact Factor of Scimago Journal and Country Rankings (Rosário, 2022).

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

The International Journal of Information Management stands out as the most frequently cited publication, boasting an SJR of 2.770, a Q1 ranking, and an H index of 114. Among the 48 journal titles, there are seven in Q1, four in Q2, seven in Q3, and five in Q4. The top quartile, Q1, accounts for 15% of the total, while Q2 represents 8%, Q3 also 15% and Q4 10%. Notably, data for 25 of the 48 journals, which constitutes 52%, is unavailable.

As illustrated in Table 3, a significant portion of articles addressing cybersecurity within the Internet of Things in Industrial Management is found in the Q1 category. The 60 scientific articles span various subject areas, including 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 cited article, titled "Blockchain technology innovations," received 155 citations and was published in the 2017 IEEE Technology and Engineering Management Society Conference (TEMSCON 2017), which has an SJR of 0.210 and is yet to be assigned a quartile, with an H index of 6. This article highlights the application of Blockchain technology across various industrial sectors. Figure 2 presents an analysis of citation trends for articles published from 2014 to 2021, revealing a positive growth trajectory with an R2 of 80% during this period, peaking at 217 citations in 2020 (Rosário, 2022).

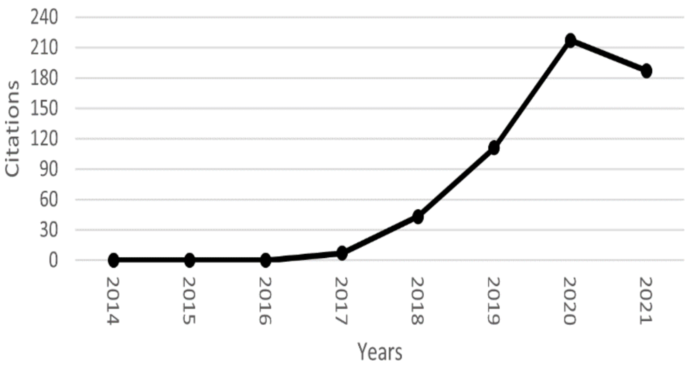

Figure 2. Evolution of citations between 2014 and 2021 (Rosário, 2022).

The H index was employed to evaluate the productivity and influence of published works, determined by the highest number of articles that received a minimum number of citations. Among the documents analyzed for the H index, 10 were cited at least 10 times.

Appendix A provides an analysis of citations for all scientific articles published between 2014 and 2021, totaling 568 citations; out of 60 publications, 19 were not cited. Appendix B focuses on self-citation trends from 2014 to 2021, revealing that 20 documents were self-cited 48 times. Notably, the article titled "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," received 10 citations.

Figure 3 presents a bibliometric analysis aimed at exploring the evolution of scientific knowledge through key terms. This bibliometric output, generated using the scientific software VOSviewer, seeks to highlight the primary research keywords "Cyber Security" and "Internet of Things."

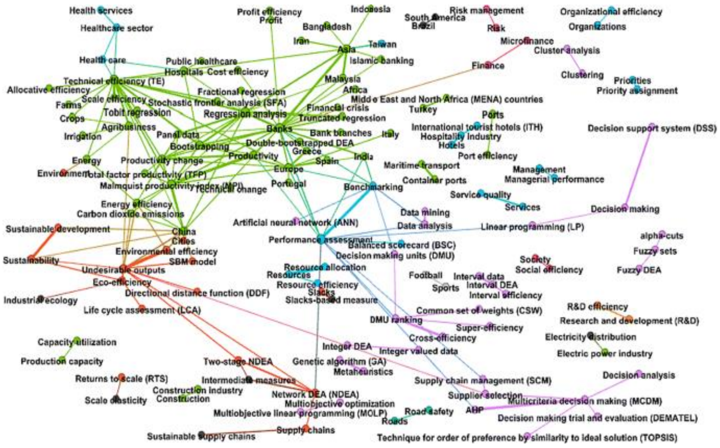

Figure 3. Network of all keywords (S. Lozano, 2019).

The study was based on a review of articles focused on consumer marketing strategies in e-commerce over the past ten years. Figure 4 presents the related keywords, depicting the network of terms that are frequently associated within each scientific article.

This visualization aids in understanding the topics explored, which can help identify emerging research trends. Additionally, Figure 5 demonstrates the co-citation relationships within the analyzed references.

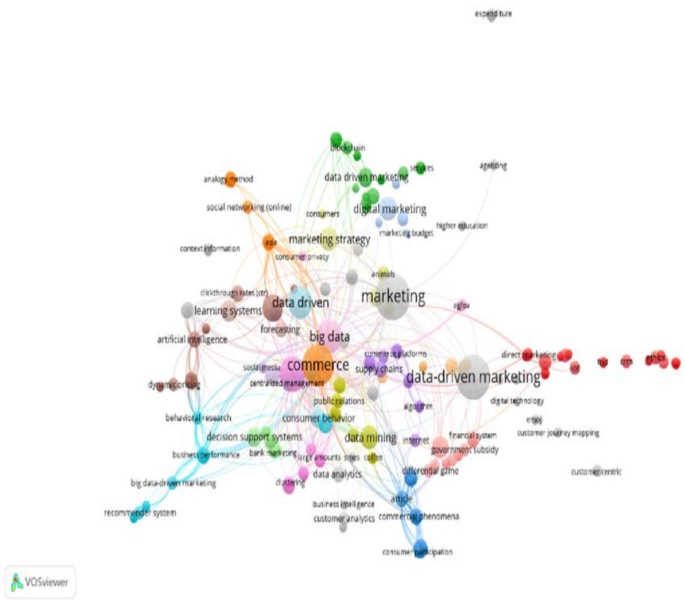

Figure 4. Network of linked keywords (Rosário Albérico, 2024).

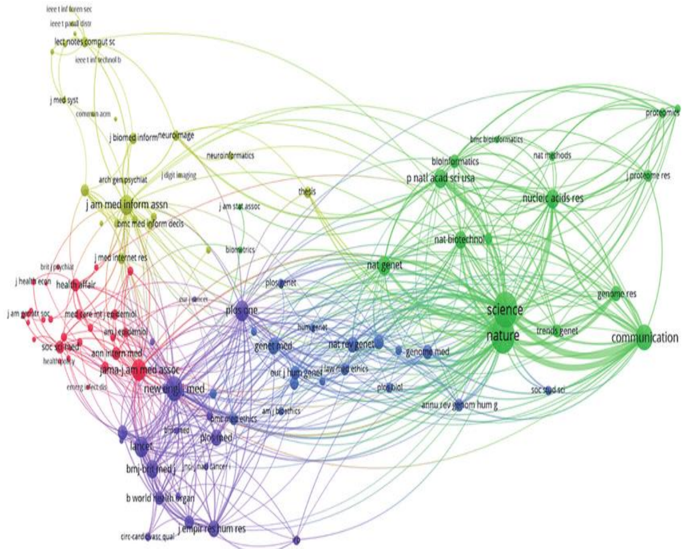

Figure 5. Networks of co-citation (Vincent Le Texier, 2019).

4. Discussion

The previously mentioned subjects concerning cybersecurity within the Industrial Internet of Things (IIoT) appear in academic literature as separate subthemes, including machine learning and cloud computing, with various applications focused on security. These concepts have been extensively utilized to address significant challenges and to showcase leading authors, notably Ahram (Ahram, Sargolzaei, Sargolzaei, Daniels, & Amaba, 2017) and Ardito (Ardito, Petruzzelli, Panniello, & Garavelli, 2018) (see Figure 5). The primary themes that highlight the ongoing discussion are depicted in Figures 3 and 4 and warrant further attention.

4.1. Cybersecurity

Cybersecurity has primarily concentrated on safeguarding specific data against both physical and cloud-based threats. It addresses the risks posed to digital infrastructure and is crucial for sustaining business growth in an environment characterized by evolving technologies in the social, mobility, analytics, and cloud (SMAC) sectors, as well as the Internet of Things (IoT). This evolution necessitates the development of new cybersecurity capabilities (Dube & Mohanty, 2020). The focus is on users' vulnerability to cyber-attacks and how various factors, such as user proficiency in managing online threats, influence this relationship within the IoT context (Albladi & George, 2017). It highlights significant threat drivers and identifies emerging technologies, including encryption and Blockchain, that could affect both defensive and offensive capabilities in cybersecurity (Yoel Raban, 2018).

The current body of literature also points to key platforms that can support smart objects, such as smart home systems that connect sensors, which are at risk of identity theft and require protection (Alshboul, Bsoul, Zamil, & Samarah, 2021). It addresses the challenges of securing automated power consumption devices that utilize smart technology in IoT environments (Sivakumar, Siddappa Naidu, & Karunanithi, 2019) and reviews essential technologies, best practices, policies, and security frameworks across various countries, involving stakeholders from government, industry, civil society, and academia (Sayed-Mouchaweh, 2020). Lastly, some studies explore the justification of cybersecurity laws, particularly in countries like China that may require a more robust cybersecurity framework (Parasol, 2018).

4.2. Machine Learning

The topic of machine learning, which encompasses artificial intelligence, is intricately linked to cybersecurity. This area emphasizes the use of intelligence in energy management, particularly in production systems, while addressing cybersecurity challenges within Industry 4.0 and the Internet of Things (Sayed-Mouchaweh, 2020). A significant focus is placed on the relationship between feature selection and interpretation within the machine learning process, particularly for intrusion detection in IoT networks (Nomm, Guerra-Manzanares, & Bahsi, 2019). AI techniques are frequently employed to identify cyber-attacks in various internet-connected environments, such as smartphones and robotic manufacturing facilities, and to facilitate decision-making during incidents through data mining methods, enhancing cyber defense strategies (Gupta, Sabitha, & Punhani, 2019). Additionally, there are efforts to integrate AI into business practices, promoting the adoption of rational, relevant, and practical strategies across various enterprise functions, including emerging technologies like IoT, Blockchain, and cloud computing (Mohanty & Vyas, 2018).

4.3. The Internet of Things (IoT)

The Internet of Things (IoT) plays a pivotal role in this discussion, significantly affecting both the industrial sector (IIoT) and the realms of network and cloud computing. This topic has highlighted the necessity for intrusion detection systems capable of safeguarding data and physical devices. These systems utilize artificial intelligence to create an intelligent intrusion detection model that identifies threats, employing Decision Trees for network intrusion detection (Al-Omari, Rawashdeh, Qutaishat, Alshira'H, & Ababneh, 2021). Furthermore, it empowers individuals in households to manage intelligent IoT agents within their personal environments (Oravec, 2017), while enabling executives to adopt a dynamic Extended Risk-Based Approach for securing enterprises in the context of cloud and IoT (Griffy-Brown, Miller, Zhao, Lazarikos, & Chun, 2019). This approach is relevant to virtually all paperless work settings (Cˇapek, 2018), addressing threats such as distributed denial of service (DDoS) attacks on power grids and the hacking of industrial control systems, along with the subsequent regulatory measures (Lachlan Urquhart, 2018).

Additionally, IoT theory investigates how the entire supply chain can gain from the integration of 4.0 technologies, providing the agility that customers demand and leveraging big data, cloud computing, and cybersecurity through enhanced communication systems (Dalmarco & Barros, 2018). For instance, it seeks to evaluate device and network security while exploring various scenarios involving different attackers intent on compromising the IoT wireless network (Ivan Vaccari, 2019), as well as applying learning curves to significant global cyber incidents (Gary, Marinakis, Majadillas, White, & Walsh, 2019).

Another area of research focuses on the technologies being implemented and the organizational risks being assessed, developing a risk model that addresses AI, IoT, and distributed ledger technologies (Griffy-Brown, Miller, Zhao, Lazarikos, & Chun, 2019). This literature also provides an in-depth examination of trust management models designed to enforce various security protocols within IoT systems, ensuring the safety of connected devices (Murshida, Faizabadi, Basthikodi, & Akram, 2019). This encompasses technologies like augmented reality (AR), which bridges the gap between the physical and virtual realms, aimed at establishing guidelines for Industry 4.0 (Rafaqat, Ishfaq, & Ahmed, 2019), tourism, business integration, and essential performance metrics (Rua-Huan Tsaih, 2018).

The Internet of Things (IoT) incorporates a wide array of smart devices interconnected through networks, necessitating safety for both physical entities and individuals, as well as security for data and IT infrastructures. Efforts are underway to enhance security within the automotive sector by creating an encryption system designed to obscure data from unauthorized users and to identify actions that could jeopardize vehicle integrity. Specifically, an intrusion detection system is being developed to monitor traffic on the Controller Area Network (CAN-Bus) and to discern whether the transmitted messages are harmful (Pascale, Adinolfi, Coppola, & Santonicola, 2021), (Lombardi, Pascale, & Santaniello, 2022), (Lu & Xu, 2018).

Additionally, it is important to highlight the cybersecurity challenges faced by electric vehicles (EVs), particularly in recognizing critical issues that have been identified but not adequately addressed in terms of cybersecurity requirements (Khalid, 2019), such as those related to EV battery stacks. Strategies are proposed for the automotive industry to mitigate cybersecurity threats. Similarly (Morris, Madzudzo, & Garcia-Perez, 2018), research has been conducted on the security weaknesses of unmanned vessels, outlining potential defense strategies and countermeasures (Silverajan, Ocak, & Nagel, 2018), while also addressing the vulnerabilities present in the wireless systems of software-defined radios (Hitefield, Fowler, & Clancy, 2019).

In conclusion, the increasing prevalence of smart devices is accompanied by a rise in associated risks, both for individual users and the broader Internet, particularly concerning hacking threats (Nash, 2021). However, there is a notable absence of clear policy guidance, a misunderstanding of user priorities regarding cybersecurity, and ambiguity surrounding the development of IoT public policy, especially in relation to stakeholder values (Smith, 2021). Furthermore, there is a pressing need for a new proactive antifragility paradigm in cyber defense strategies tailored for the IoT landscape, particularly within complex distributed computing environments that extend beyond conventional cyber defense mechanisms, such as the Internet of Battle Things (IoBT) (Uzunov, Nepal, & Chhetri, 2019), to effectively address emerging threats (Sahu, Sahu, & Sahu, 2020).

Additionally, various solutions have been proposed to tackle new wireless challenges, including 6G technology, dynamic spectrum access (DSA) (Akyildiz, Lee, Vuran, & Mohanty, 2006), and wireless mesh networks (WMNs) (Akyildiz, Wang, & Wang, Wireless mesh networks: A survey, 2005). This shift aims to transition from the Internet of Things (IoT) to the Internet of Intelligence (IoI), enhancing connectivity while enabling autonomous knowledge processing and decision-making (Soldani, 2021). The goal is to create innovative methodologies for fingerprinting IoT devices through data-driven techniques based on machine learning, which can help identify compromised IP addresses across different geographical regions (Mangino, Pour, & Bou-Harb, 2020). Moreover, the current lack of robust IoT cyber risk management frameworks and effective sensor networks (Akyildiz, Su, Sankarasubramaniam, & Cayirci, 2002) raises concerns about distributed denial of service (DDoS) attacks, particularly in the healthcare sector where security is often limited (Khatkar Monika, 2020), while also necessitating an examination of the evolving legal landscape within the IoT regulatory framework (Weber & Studer, 2016).

4.4. Industrial Internet of Things (IIoT)

Industry 4.0 represents a significant subtheme within the realm of the Internet of Things (IoT), often referred to as the Industrial Internet of Things (IIoT). Various studies explore the impact of essential technologies such as artificial intelligence, big data, and augmented reality on the circular economy, particularly in areas like recycling and minimizing waste and emissions. This underscores the vital role of Industry 4.0 in enhancing circularity (Iker Laskurain-Iturbe, 2021). Additionally, some research highlights the influence of these digital technologies on e-finance, presenting opportunities for transforming business models (Dandapani, 2017), particularly through the application of AI. This includes the development of technologies aimed at managing the intersection of supply chain management and marketing processes, thereby supporting the integration of supply chain management and marketing (SCM-M) (Ardito, Petruzzelli, Panniello, & Garavelli, 2018). Furthermore, there is a focus on the oil and gas sector, addressing concerns regarding the migration of sensitive business data to cloud-based digital platforms, which encompasses decision-making processes and procedures (Chaykin, 2019), as well as the increased entry points for organizations to bolster their defenses against potential threats (Culot, Fattori, Podrecca, & Sartor, 2019).

Another area of research identifies gaps within Industry 4.0, utilizing an open internet-based research search engine to obtain digital object identifiers and universal resource locators when DOIs are unavailable for research articles (Sahu, Sahu, & Sahu, 2020). Current discussions revolve around concepts such as the smart factory, which leverages ICT technology to reduce manufacturing costs and time, while also emphasizing the need to mitigate security vulnerabilities (Lee, Kim, & Kim, 2019). Additionally, securing electro-energy platforms is highlighted as a critical requirement for ensuring a safe monitoring and control system for electric vehicle charging (Terruggia & Garrone, 2020).

The primary concern revolves around how cybersecurity addresses cyber threats in the context of Industry 4.0, particularly in relation to contemporary topics such as cloud computing, smart grids, intrusion detection, privacy, the Internet of Things, and smart cities (Furstenau, et al., 20 years of scientific evolution of cyber security:, 2020). It is essential to adapt to the ongoing technological transformation while implementing strategies to mitigate potential severe impacts across various sectors, including e-commerce and banking. Additionally, it is crucial to focus on navigating digitalization with a customer-centric approach among diverse manufacturers (Sarı, Güle¸s, & Yi ˘ gitol, 2020). Ultimately, the Fourth Industrial Revolution will bring about significant economic, social, and political ramifications on a global scale, resulting in transformative changes in the intelligent production of goods and services, alongside increasing unemployment and social inequality (Rymarczyk, 2020).

4.5. Blockchain and Cloud Computing

The discussion surrounding the decentralized architectures of IoT devices is currently prominent. Recent advancements in Blockchain technologies have facilitated the creation of a smart ecosystem that supports cybersecurity measures across various sectors, including smart home installations. This ecosystem emphasizes the immutability of both users and devices, as well as the dynamic management of blocked malicious IP addresses (K. M. Giannoutakis, 2020). It finds applications in numerous fields such as industrial operations, healthcare, finance, and government (Ahram, Sargolzaei, Sargolzaei, Daniels, & Amaba, 2017), addressing cybersecurity challenges related to accountability, traceability, and identification (Gorog Christopher, 2018).

A critical aspect of this discourse is enhancing the security of system architectures to safeguard against malicious internal users and malware embedded within the system. This challenge can be addressed through a robust sensor network (Akyildiz, Su, Sankarasubramaniam, & Cayirci, 2002), which is integral to Blockchain's security framework (Kis & Singh, 2018). Blockchain technology can enhance the privacy, security, and non-repudiation of IoT systems by managing the vast amounts of data generated and the diverse sensors and devices utilized (Occa, Borbon-Galvez, & Strozzi, 2020). It enables the development of a scalable and decentralized end-to-end secure IoT infrastructure (Najmeddine Dhieb, 2020). Additionally, integrating AI at the gateway level can further improve the IoT by enabling the detection and classification of suspicious activities. Furthermore, Blockchain technology can be effectively combined with cloud computing in higher education, particularly in establishing foundational infrastructure that integrates machine learning and artificial intelligence for training purposes (Foster, et al., Toward a cloud computing learning community. In ITiCSE-WGR ’19, Proceedings of the Annual Conference on Innovation and Technology in Computer Science Education, 2019).

Cloud computing is closely linked to Blockchain technology, particularly in its ability to safeguard against attacks targeting radio-frequency (RF)-enabled devices, Internet of Things (IoT) firmware, and wireless communication protocols (Oconnor & Stricklan, 2021). The integration of smart devices and reliance on public networks are central issues in the discourse surrounding smart cities, where interconnected services for residents raise significant cybersecurity concerns (Grandhi, Grandhi, & Wibowo, 2021). These concerns encompass various areas, including communication infrastructures, cloud computing, smart healthcare, and energy management (Ismail & Zhang, 2017).

The conversation around cloud computing also addresses the cybersecurity of supply chains reliant on software and networks, aiming to reduce the risks associated with the procurement and disconnection of critical machinery from networks (Latif, et al., 2015). In conclusion, while 5G and 6G networks promise innovative communication infrastructure, IoT systems will continue to present vulnerabilities that hackers can exploit. Therefore, there is an urgent need for systems capable of detecting and mitigating potential threats in next-generation networks and decentralized frameworks like Blockchain (Ghorbani, Mohammadzadeh, & Ahmadzadegan, 2020).

5. CONCLUSIONS

The Internet of Things (IoT) plays a crucial role in various sectors, including smart manufacturing, smart cities, smart healthcare, smart grids, and electric vehicles. By connecting physical devices to the Internet, both in everyday life and industrial settings, IoT and Industrial IoT (IIoT) create numerous opportunities. However, this connectivity also raises concerns about the security of sensitive data and critical infrastructure, making them vulnerable to potential hacking. Moreover, the vast amounts of data generated by IoT systems present significant security challenges due to their interconnected nature, whether through cloud computing or Blockchain technologies in smart factories, homes, and cities. Therefore, it is essential for cybersecurity efforts to prioritize the diverse vulnerabilities associated with IoT devices and enhance security measures, including privacy, access control, data storage, and authorization. Organizations must develop a robust cybersecurity strategy to keep pace with technological advancements and effectively address emerging threats. This study contributes to the existing literature on IIoT cybersecurity by thoroughly examining its key subtopics and promoting further exploration in this area. Additionally, emerging technologies like Blockchain are expected to play a pivotal role in the future of IoT and IIoT cybersecurity, as the proliferation of wireless-connected devices necessitates improved security management across all aspects of daily life.

ACKNOWLEDGEMENT

We wish to extend our sincere appreciation to the editor and the referees for their invaluable suggestions and enhancements. The authors received support from the GOYCOPP Research Unit at Universidad de Aveiro and ISEC Lisboa, Higher Institute of Education and Sciences.

REFERENCES

(n.d.). Retrieved from https://www.geeksforgeeks.org/architecture-of-internet-of-things-iot/

Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J., & Amaba, B. (2017). B. Blockchain technology innovations. *In Proceedings of the 2017 IEEE Technology and Engineering Management Society Conference (TEMSCON),*, (pp. 137–141). Santa Clara, CA, USA,.

Akyildiz, I., Lee, W.-Y., Vuran, M., & Mohanty, S. (2006). NeXt generation/dynamic spectrum access/cognitive radio wireless networks A survey. 2127–2159.

Akyildiz, I., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). Wireless sensor networks: A survey. 393–422.

Akyildiz, I., Wang, X., & Wang, W. (2005). Wireless mesh networks: A survey. 445–487.

Albladi, S., & George, R. (2017). Personality traits and cyber-attack victimisation: Multiple mediation analysis. *In Proceedings of the 2017 Internet of Things–Business Models, Users, and Networks, Copenhagen, Denmark*.

Alejandro Guerra-Manzanares, S. N. (2019). Towards the Integration of a Post-Hoc Interpretation Step into the Machine Learning Workflow for IoT Botnet Detection. *International Conference on Machine Learning and Applications (ICMLA)*, 1162–1169.

Al-Omari, M., Rawashdeh, M., Qutaishat, F., Alshira'H, M., & Ababneh, N. (2021). An intelligent tree-based intrusion detection model for cyber security. 20.

Alshboul, Y., Bsoul, A., Zamil, M., & Samarah, S. (2021). Cybersecurity of smart home systems: Sensor identity protection. 22.

Arbia Riahi Sfar a b, E. N. (2017). A roadmap for security challenges in the Internet of Things.

Ardito, L., Petruzzelli, A., Panniello, U., & Garavelli, A. (2018). Towards industry 4.0: Mapping digital technologies for supply chain management-marketing integration. 323–346.

Biljana L. Risteska Stojkoska, K. V. (2017, January 1). A review of Internet of Things for smart home: Challenges and solutions. *Journal of Cleaner Production, 140*, 1454-1464.

Cˇapek, J. (2018). Cybersecurity and internet of things. *In Proceedings of the IDIMT 2018 Strategic Modeling in Management, Economy and Society–26th Interdisciplinary Information Management Talks*, 343–349.

Chaykin, A. (2019). New systems, new cyber threats. 32–33.

Culot, G., Fattori, F., Podrecca, M., & Sartor, M. (2019). Addressing industry 4.0, cybersecurity challenges. 79–86.

Dalmarco, G., & Barros, A. M. (2018). Adoption of industry 4.0 technologies in supply chains. *Springer: Cham*.

Dandapani, K. (2017). Electronic finance–recent developments. 614–626.

Dube, D., & Mohanty, R. (2020). Towards development of a cyber security capability maturity model. 104–127.

Foster, D., White, L., Erdil, D., Adams, J., Argüelles, A., Hainey, B., . . . al., e. (2019). Toward a cloud computing learning community. 143–155.

Foster, D., White, L., Erdil, D., Adams, J., Argüelles, A., Hainey, B., . . . al., e. (2019). Toward a cloud computing learning community. In ITiCSE-WGR '19, Proceedings of the Annual Conference on Innovation and Technology in Computer Science Education., (pp. 143–155). New York, NY, USA.

Furstenau, L., Sott, M., Homrich, A., Kipper, L., Al Abri, A., Cardoso, T., . . . Cobo, M. (2020). 20 years of scientific evolution of cyber security. *A science mapping. In Proceedings of the International Conference on Industrial Engineering and Operations Management, Dubai, United Arab Emirates*, 314–325.

Furstenau, L., Sott, M., Homrich, A., Kipper, L., Al Abri, A., Cardoso, T., . . . Cobo, M. (2020). 20 years of scientific evolution of cyber security:. 314–325.

Gary, R., Marinakis, Y., Majadillas, M., White, R., & Walsh, S. (2019). Legitimate firms or hackers–who is winning the global cyber war? *Int. J. Technol. Intell. Plan.*, 297–314.

Ghorbani, H., Mohammadzadeh, M., & Ahmadzadegan, M. (2020). Modeling for malicious traffic detection in 6G next generation networks. *In Proceedings of the 2020 International Conference on Technology and Entrepreneurship–Virtual (ICTE-V)*, (pp. 20–21). San Jose,CA, USA,.

Gorog Christopher, T. E. (2018). Solving Global Cybersecurity Problems by Connecting Trust Using Blockchain.

Grandhi, L., Grandhi, S., & Wibowo, S. (2021). A security-UTAUT framework for evaluating key security determinants in smart city adoption by the australian city councils. In Proceedings of the 2021 21st ACIS International Semi-Virtual Winter Conference on Software Engineering, Artificial Intelligence. 17–22.

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? *In Proceedings of the 2019 IEEE Technology and Engineering Management Conference (TEMSCON)*, (pp. 12–14). Atlanta, GA, USA.

Gupta, R. (2021). Industry 4.0 adaption in indian banking Sector—A review and agenda for future research.

Gupta, S., Sabitha, A., & Punhani, R. (2019). Cyber security threat intelligence using data mining techniques and artificial intelligence. 6133–6140.

Hitefield, S., Fowler, M., & Clancy, T. (2019). Exploiting buffer overflow vulnerabilities in software defined radios. In Proceedings of the 2018 IEEE Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber. *Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData),*, (pp. 1921–1927). Halifax, NS, Canada.

Iker Laskurain-Iturbe, G. A.-L.-M.-G. (2021). Exploring the influence of industry 4.0 technologies on the circular economy. *321*, 128944.

Ismail, L., & Zhang, L. (2017). Information Innovation Technology in Smart Cities. 1–356.

Ivan Vaccari, E. C. (2019). Evaluating Security of Low-Power Internet of Things Networks. *International Journal of Computing and Digital Systems 8(2):*, 101-114.

K. M. Giannoutakis, G. S.-P. (2020). A Blockchain Solution for Enhancing Cybersecurity Defence of IoT. *2020 IEEE International Conference on Blockchain, Blockchain 2020*, 490-495.

Khalid, A. S. (2019). Facts approach to address cybersecurity issues in electric vehicle battery systems. In 2019 IEEE Technology & Engineering Management Conference (TEMSCON) . 1-6).

Khatkar Monika, K. K. (2020). An overview of distributed denial of service and internet of things in healthcare devices.

Kis, M., & Singh, B. (2018). A cybersecurity case for the adoption of blockchain in the financial industry. *In Proceedings of the 2018 IEEE Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData*, 1491–1498.

Kouicem, D. E. (2018). Internet of Things Security: a top-down survey. *141*.

Lachlan Urquhart, D. M. (2018, June). Avoiding the internet of insecure industrial things. *Computer Law & Security Review, 34*, 450-466.

Latif, M., Sarawak, S., Aziz, N., Hussin, N., Aziz, Z., & Kelantan, K. (2015). Cyber security in supply chain management. *A systematic review*, 49–57.

Lee, T., Kim, S., & Kim, K. (2019). A research on the vulnerabilities of PLC using search engine. In Proceedings of the 10th International. *ICT Convergence Leading the Autonomous Future*, 184–188.

Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications.

Lombardi, M., Pascale, F., & Santaniello, D. (2022). Two-Step Algorithm to Detect Cyber-Attack Over the Can-Bus: A Preliminary Case Study in Connected Vehicles. 031105.

Lu, Y., & Xu, L. (2018). Internet of Things (IoT) cybersecurity research: A review of current research topics. 2103–2115.

Mangino, A., Pour, M., & Bou-Harb, E. (2020). Internet-scale insecurity of consumer internet of things. 1–24.

Memon, K., & Ooi, S. (2021). The Dark Side of Industrial Revolution 4.0-Implications and Suggestions., (pp. 1–18).

Michele Kremer Sott*, L. B.-R. (2020). Precision Techniques and Agriculture 4.0 Technologies to Promote Sustainability in the Coffee Sector: State of the Art, Challenges and Future Trends. 14.

Mohammad Al-Omari, M. R. (2021). An Intelligent Tree-Based Intrusion Detection Model for Cyber Security. *Journal of Network and Systems Management* , 29,20.

Mohanty, S., & Vyas, S. (2018). How to Compete in the Age of Artificial Intelligence: Implementing a Collaborative Human-Machine Strategy for. 1–229.

Morris, D., Madzudzo, G., & Garcia-Perez, A. (2018). Cybersecurity and the auto industry: The growing challenges presented by connected cars. 105–118.

Muhammad Shoaib Farooq, M. A. (n.d.).

Murshida, Faizabadi, A., Basthikodi, M., & Akram, K. (2019). Trust management in internet of things applications. *Int. J. Recent Technol.Eng.*, 1750–1753.

Najmeddine Dhieb, H. G. (2020). Scalable and Secure Architecture for Distributed IoT Systems. *2020 IEEE Technology & Engineering Management Conference (TEMSCON).*

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*, 105529.

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. *In Proceedings of the 18th IEEE International Conference on Machine Learning and Applications (ICMLA),*, (pp. 1162–1169). Boca Raton, FL, USA,.

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.

Oconnor, T., & Stricklan, C. (2021). Teaching a hands-on mobile and wireless cybersecurity course. *In ITiCSE '21, Proceedings of the ACM Conference on Innovation and Technology in Computer Science Education, Virtual Event*, (pp. 296–302). Germany.

Oravec, J. (2017). Kill switches, remote deletion, and intelligent agents. *Framing everyday household cybersecurity in the internet of things*, 189–198.

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 & Security Review, 34*, 67–98.

Pascale, F., Adinolfi, E., Coppola, S., & Santonicola, E. (2021). Cybersecurity in Automotive: AnIntrusion Detection System in Connected Vehicles. 1765.

Rafaqat, M., Ishfaq, K., & Ahmed, N. (2019). Implementation of augmented reality in the context of industry 4.0: A comprehensive review. *In Proceedings of the 9th Annual International Conference on Industrial Engineering and Operations Management*, 3–94.

Rosário Albérico, J. C. (2024). Relationship Marketing and Customer Retention - A Systematic Literature Review. 44-66.

Rosário, R. J. (2022). Cybersecurity in the Internet of Things in. 5-9.

Rua-Huan Tsaih, C. C. (2018). Artificial Intelligence in Smart Tourism: A Conceptual Framework . *In Proceedings of The 18th International Conference on Electronic Business*, 124-133.

Rymarczyk, J. (2020). Technologies, opportunities and challenges of the industrial revolution 4.0: Theoretical considerations. 185–198.

S. Lozano, L. C.-I.-D. (2019). Complex network analysis of keywords co-occurrence in the recent efficiency analysis literature. 609–629.

Sahu, A., Sahu, A., & Sahu, N. (2020). A review on the research growth of industry 4.0: IIoT business architectures benchmarking. *Int. J. Bus. Anal*, 77–97.

Salman, T., Zolanvari, M., Erbad, A., Jain, R., & Samaka, M. (2018). Security services using blockchains: A state of the art survey.

Sarı, T., Güle¸s, H., & Yi ˘ gitol, B. (2020). Awareness and readiness of industry 4.0: The case of turkish manufacturing industry. 57–68.

Sayed-Mouchaweh, M. (2020). Artificial Intelligence Techniques for a Scalable Energy Transition. *Advanced Methods, Digital Technologies,Decision Support Tools, and Applications*, 1–382.

Silverajan, B., Ocak, M., & Nagel, B. (2018). Cybersecurity attacks and defences for unmanned smart ships. *In Proceedings of the 2018 IEEE Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 15–20.

Sivakumar, S., Siddappa Naidu, K., & Karunanithi, K. (2019). Design of energy management system using autonomous hybrid micro-grid under IOT environment. *Int. J. Recent Technol. Eng*, 338–343.

Smith, K. J. (2021, February). User values and the development of a cybersecurity public policy for the IoT. *International Journal of Information Management*, pp. 2-3.

Soldani, D. (2021). 6G Fundamentals: Vision and Enabling Technologies. 58–86.

T. Ahram, A. S. (2017). Blockchain technology innovation. *EEE Technology & Engineering Management Conference (TEMSCON*, 137-141.

Terruggia, R., & Garrone, F. (2020). Secure IoT and cloud based infrastructure for the monitoring of power consumption and asset control. *In Proceedings of the 12th AEIT International Annual Conference (AEIT)*, (pp. 23–25). Catania, Italy.

Uzunov, A. V., Nepal, S., & Chhetri, M. B. (2019). Proactive Antifragility: A New Paradigm for Next-Generation Cyber Defence at the Edge. *2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC).*

Vincent Le Texier, N. H.-T. (2019). Data sharing in the era of precision medicine: A scientometric analysis. 30-30.

Weber, R., & Studer, E. (2016). Cybersecurity in the internet of things. *Legal aspects. Comput. Law Secur. Rev*, 715–728.

Yoel Raban, A. H. (2018). Foresight of cyber security threat drivers and affecting technologies. 353–363.

BIOGRAPHIES

Sachin Vasant Dorage Lead System Administrator Information Technology Oriental College of Pharmacy, Navi Mumbai, Maharashtra, India

Appendix A

Table A1. Overview of document citations from 2014 to 2021 (Rosário, 2022).

Documents		**2014**	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**	**2021**	**Total**
An Intelligent Tree-Based Intrusion Detection Model for Cyber...	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 Defense 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
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	0	0	0	7	43	111	217	187	568

Appendix B

Table A2. Overview of document self-citations from 2014 to 2021 (Rosário, 2022).

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