ISSN 2007-9737

Systematic Literature Review on Cybersecurity and its Influence on Cyber Attacks Targeting IoT Devices

Mario Padilla-Gomez[1*], Javier Gamboa-Cruzado[2], Segundo Távara-Aponte[5], Ángel Núñez-Meza[3], Flavio Amayo-Gamboa[4], Saul Arauco-Esquivel[6]

[1] Universidad Nacional Federico Villarreal, Facultad de Ingeniería Industrial y de Sistemas, Lima, Peru

[2] Universidad Nacional Mayor de San Marcos, Facultad de Ingeniería de Sistemas e Informática, Lima, Peru

[3] Universidad Nacional Daniel Alcides Carrión, Facultad de Ingeniería de Sistemas, Pasco, Peru

[4] Universidad Nacional de Trujillo, Escuela de Informática, Trujillo, Peru

[5] Universidad Nacional de Trujillo, Facultad de Ciencias Físicas y Matemáticas, Trujillo, Peru

[6] Universidad Nacional Mayor de San Marcos, Facultad de Ingeniería Geológica, Minera, Metalúrgica y Geográfica, Lima, Peru

2017022321@unfv.edu.pe, jgamboa65@hotmail.com, {stavara, famayo}@unitru.edu.pe, anunezm@undac.edu.pe, saraucoe@unmsm.edu.pe

Abstract. The Internet of Things (IoT) offers a valuable proposition for various sectors of society, ranging from light bulbs to healthcare resources and even smart city infrastructures. This technology interacts with a considerable volume of data, which is susceptible to potential alterations or thefts. Consequently, one of the main challenges in cybersecurity involves preventing, detecting, and managing these incidents. The aim of this study is to establish the current state of knowledge regarding cybersecurity and its influence on cyber-attacks directed at IoT devices. In this context, a systematic review of empirical studies up to the year 2022 was conducted. The search strategy resulted in the identification of 70 studies, which were subjected to exclusion criteria and evaluated in terms of quality to form the definitive list. The selected studies were organized into a PRISMA diagram and categorized according to sources of information such as Scopus, Web of Science, IEEE Xplore, EBSCOhost, ARDI, and ProQuest. The results of the systematic review revealed four criteria for measuring the effectiveness of cybersecurity and highlighted China, the United Kingdom, and the United States as the most productive countries in terms of the number of published papers and collaborations. This study provides valuable information for future research and establishes a point of comparison across different situational environments.

Keywords. Systematic literature review, cybersecurity, internet of things, IoT devices, cyber-attacks.

1 Introduction

The rapid technological development has increased the presence of IoT (Internet of Things) devices in our daily lives, turning them into common elements that facilitate internet connectivity and intercommunication to enhance our quality of life and optimize efficiency across various fields.

Efficient data management in diverse devices such as apparel with integrated technology, smartwatches, intelligent bracelets, portable medical devices, and other consumer services within the IoT spectrum is essential [84].

The data collected by these devices are amalgamated to provide detailed information to users through the network, fulfilling the objectives for which they were designed. However, connectivity also introduces significant inherent security risks. Cyber attacks on IoT devices are becoming increasingly frequent and complex, representing a considerable challenge for digital security.

To counter these risks, cybersecurity is essential. Both users and manufacturers of IoT devices must adopt measures to protect their devices against cyber threats, including the implementation of robust passwords, regular software updates, and appropriate privacy settings. Given the wide range of services they offer, the sensors in IoT devices generate large volumes of data that require authentication, security, and privacy [71].

The Internet of Things (IoT) has established a new paradigm where a network of machines and devices, capable of communicating and collaborating, drives innovations in business processes [81]. This paradigm emerges from the convergence of diverse technologies, such as physical devices, vehicles, and other items equipped with electronics, software, and sensors, along with network connectivity that facilitates the collection and exchange of data from and between connected objects [76].

The interconnection of smart objects enables numerous IoT applications in various fields such as logistics, transportation, industry, and healthcare [91]. The number of IoT devices is growing exponentially, extending into diverse domains, from smaller scales like a Smart Grid to larger scales like Smart Cities [83]. Globally, IoT solutions are on the rise, and projections for the coming years are encouraging, with the number of IoT devices expected to reach between 25,000 and 30,000 million by 2022 [72]. However, the popularity of IoT devices is limited by cyberattacks and security threats.

According to an analysis by HP, common IoT devices exhibit an average of 25% vulnerabilities per device [83]. The sensitive data generated by these devices attract unauthorized third parties, posing a significant concern for end-users and businesses at the risk of losing control over their data [91].

Security and privacy in IoT remain major concerns due to the heterogeneity and natural vulnerability of devices on a large scale in operational environments [83]. Cyber attacks have rapidly increased in sectors such as smart homes, healthcare, energy, agriculture, and industrial automation [71].

The goal of cybersecurity in IoT is to minimize the risk of cyberattacks for organizations and users, protecting IoT assets and privacy [81]. Therefore, given the need for strategic decisions and investments, cybersecurity must prioritize identifying and mitigating vulnerabilities in IoT objects, focusing on privacy, access control, data storage, and adopting a comprehensive cybersecurity strategy [86].

In this context, the need to understand the risks associated with IoT devices and the importance of cybersecurity to prevent cyber attacks is highlighted. This review can contribute to identifying gaps in the existing literature and establishing a solid foundation for future research and practices in security.

The objective of this paper is to conduct a study of the research published in the scientific literature on the topic and, through this, to answer a series of questions formulated in the methodology.

2 Theoretical Background

Given the characteristics of both cybersecurity and the threats to IoT devices, it is necessary to understand the concepts discussed before moving on to the main current trends on the issue.

2.1 Cybersecurity

Cybersecurity has been widely used in various applications such as smart industrial systems, homes, personal devices, and automobiles, and has led to innovative developments that continue to face challenges in solving security method-related issues for IoT devices [9].

Cybersecurity has become a major concern as we know that many of our everyday objects can be connected to the internet, which is fundamental in our daily lives. If it can be connected, it can be accessed. Therefore, the main concern in cybersecurity is based on intruder detection, where physical or cloud computing activities are monitored by analyzing system vulnerabilities and activity patterns [84].

Research [90] provides a systematic literature review of new techniques to counter cybercrime, given the new context of the Covid-19 pandemic. Additionally, there have been significant leaps in the use of ICT and thus, new cybercrime threats have also emerged.

2.2 Cyber Attacks on IoT Devices

IoT is a system of interconnection among computer devices, machines, objects, animals, and even people, endowed with unique identifiers capable of transferring data over a network. It utilizes integrated sensors, processors, and communication hardware to send and receive data [76]. Raimundo [84] tells us that the Internet of Things (IoT) can be described as a new topic that encompasses both the predominant internet and physical artifacts.

We can mention smart homes, for example, referring to home automation, manufacturing systems such as industrial ones, and health in terms of hospital automation. For the authors [65], the digital revolution has substantially changed our lives, in which the Internet of Things (IoT) plays a prominent role.

However, the rapid development of IoT in most corners of life brings the emergence of various cybersecurity threats. [72] state that attackers exploit vulnerabilities to execute cyberattacks. Recent attacks have exploited vulnerabilities in IoT systems in smart cities. Five main layers in the IoT system susceptible to vulnerabilities were

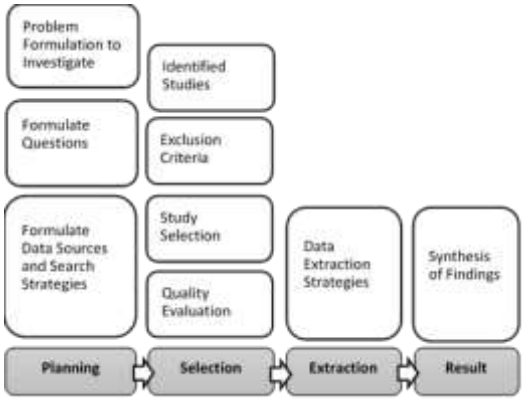

Fig. 1. Stages of an SLR

Table 1. Research questions

Research Question
RQ1: What are the criteria for measuring the effectiveness of Cybersecurity?
RQ2: Which nations lead in generating research on Cybersecurity applied to attacks on IoT devices?
RQ3: In which quartiles are the journals that disseminate research on the influence of Cybersecurity in mitigating attacks on IoT devices classified?
RQ4: How are publications that share similar conclusions in studies of Cybersecurity and its effect on attacks to IoT devices grouped?
RQ5: Which countries demonstrate frequent collaboration in research related to Cybersecurity and attacks on IoT devices?

Table 2. Search descriptors and their synonyms

Descriptor
cybersecurity / informatic security / it security / computer security / online safety / information security / / incident response / security mechanisms / cyber defense / intrusion detection / intrusion prevention
computer attack / cyberattack / network attacks / cyber threat / security incident / safety incident / cyber risk / cybercrime / iot / internet of things

identified: the network layer, the operating system, the software, the firmware, and the hardware.

3 Review Method

A systematic literature review (SLR) approach was employed following the guidelines established by B. Kitchenham [78]. The methodology used encompasses various facets: formulation of research questions, identification of data sources, search procedures, exclusion criteria, quality assessment, as well as data extraction and synthesis. The systematic review is broken down into a series of clearly delineated stages, which are illustrated in Figure 1.

3.1 Research Questions

Given the extensive nature and broad scope of research on cybersecurity in IoT devices, it is imperative to establish a search strategy that allows for efficient data extraction from each study, thereby facilitating an objective analysis to obtain relevant information. Research questions (RQ) play a crucial role in this process, which are detailed in Table 1.

3.2 Information Sources and Search Strategies

The bibliographic databases used for searching necessary research papers included IEEE Xplore, Scopus, Web of Science, ARDI, ProQuest, and EBSCOhost. The search strategy consisted of using specific keywords, as detailed in Table 2.

The search procedure was carried out using a set of terms selected to facilitate the process of exploring and abstracting information. This set of terms is called a search equation and varies depending on the information source used, as illustrated in Table 3.

3.3 Identified Studies

Upon completion of the article search in each information source, a count of the studies was obtained, which is presented in Figure 2.

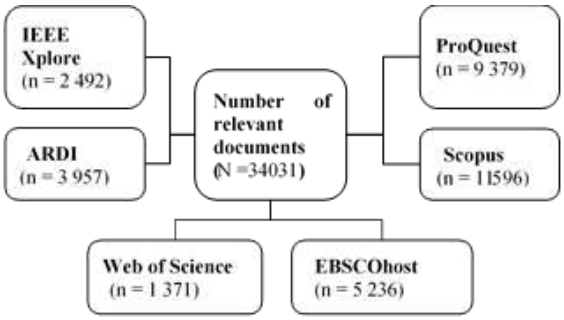

Fig. 2. Number of relevant sources

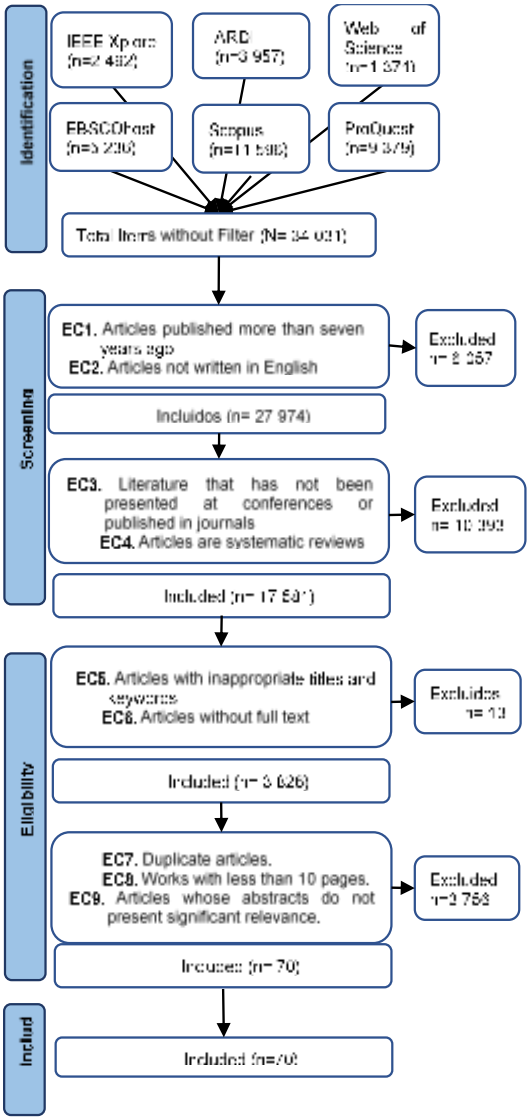

Fig. 3. PRISMA flow diagram

Table 3. Information sources and search equation

Source	Search equation
IEEE Xplore	(("Document Title": “cybersecurity” OR "Document Title": “informatic security” OR "Document Title": “it security” OR "Document Title": “computer security” OR "Document Title": “information security” OR "Document Title": “incident response” OR "Document Title": cyber defense” OR "Document Title": “intrusion detection” OR "Document Title": “intrusion prevention”) AND ("Document Title": “computer attack” OR "Document Title": “cyberattack” OR "Document Title": “network attacks” OR "Document Title": cyber threat” OR "Document Title": “security incident” OR "Document Title": “cybercrime” OR "Document Title": iot" OR "Document Title": “internet of things")) OR (("Author Keywords": cybersecurity” OR "Author Keywords": informatic security” OR "Author Keywords": “it security” OR "Author Keywords": “computer security” OR "Author Keywords": “information security” OR "Author Keywords": incident response” OR "Author Keywords": cyber defense” OR "Author Keywords": intrusion detection” OR "Author Keywords": intrusion prevention”) AND ("Author Keywords": “computer attack” OR "Author Keywords": cyberattack” OR "Author Keywords": “network attacks” OR "Author Keywords": cyber threat” OR "Author Keywords": security incident” OR "Author Keywords": cybercrime” OR "Author Keywords": iot" OR "Author Keywords": internet of things"))
ARDI	((TitleCombined:(\(“cybersecurity” \) AND \(“computer attack” OR “cyberattack” OR “network attacks” OR “cyber threat” OR “cyber risk” OR “cybercrime” OR "iot" OR "internet of things"\))) OR (Abstract:(\(“cybersecurity”\) AND \(“computer attack” OR “cyberattack” OR “network attacks” OR “cyber threat” OR “cyber risk” OR “cybercrime” OR "iot" OR "internet of things"\))))
Web of Science	(“cybersecurity” OR “informatic security” OR “it security” OR “computer security” OR “online safety” OR “information security” OR “incident response” OR “security mechanisms” OR “cyber defense” OR “intrusion detection” OR “intrusion prevention”) AND (“computer attack” OR “cyberattack” OR “network attacks” OR “cyber threat” OR “security incident” OR “cyber risk” OR “cybercrime” OR "iot" OR "internet of things") (Title) OR (“cybersecurity” OR “informatic security” OR “it security” OR “computer security” OR “online safety” OR “information security” OR “incident response” OR “security mechanisms” OR “cyber defense” OR “intrusion detection” OR “intrusion prevention”) AND (“computer attack” OR “cyberattack” OR “network attacks” OR “cyber threat” OR “security incident” OR “cyber risk” OR “cybercrime” OR "iot" OR "internet of things") (Author Keywords)
EBSCO host	TI ((“cybersecurity” OR “informatic security” OR “it security” OR “information security” OR “cyber defense”) AND (“computer attack” OR “cyberattack” OR “network attacks” OR “cyber threat” OR “security incident” OR “cyber risk” OR “cybercrime”)) OR AB ((“cybersecurity” OR “informatic security” OR “it security” OR “information security” OR “cyber defense”) AND (“computer attack” OR “cyberattack” OR “network attacks” OR “cyber threat” OR “security incident” OR “cyber risk” OR “cybercrime” OR "iot" OR "internet of things"))
Scopus	TITLE-ABS-KEY ((“cybersecurity" OR "informatic security" OR "it security" OR "computer security" OR "cyber defense" OR "intrusion detection" OR "intrusion prevention") AND ("computer attack" OR "cyberattack" OR "network attacks" OR "cyber threat" OR "security incident" OR "cyber risk" OR "cybercrime" OR "iot" OR "internet of things"))
Pro Quest	title((“cybersecurity” OR “informatic security” OR “it security” OR “computer security” OR “online safety” OR “information security” OR “incident response” OR “security mechanisms” OR “cyber defense” OR “intrusion detection” OR “intrusion prevention”) AND (“computer attack” OR “cyberattack” OR “network attacks” OR “cyber threat” OR “security incident” OR “cyber risk” OR “cybercrime” OR "iot" OR "internet of things")) OR abstract((“cybersecurity” OR “informatic security” OR “it security” OR “computer security” OR “online safety” OR “information security” OR “incident response” OR “security mechanisms” OR “cyber defense” OR “intrusion detection” OR “intrusion prevention”) AND (“computer attack” OR “cyberattack” OR “network attacks” OR “cyber threat” OR “security incident” OR “cyber risk” OR “cybercrime” OR "iot" OR "internet of things")

3.4 Selection Criteria

Exclusion criteria (EC) were established to accurately assess the quality of the retrieved literature. Articles identified will be included in the study only if they meet a list of objective exclusion criteria. To determine the final selection of articles, nine exclusion criteria were applied:

- EC1. Articles published more than seven years ago.
- EC2. Articles not written in English.
- EC3. Literature not presented at conferences or published in journals.
- EC4. Articles that are systematic reviews.
- EC5. Articles with inappropriate titles and keywords.
- EC6. Articles without full text.
- EC7. Duplicate articles.
- EC8. Works with less than 10 pages.
- EC9. Articles whose abstracts do not present significant relevance.

3.5 Study Selection

Originally, 34,031 articles were obtained based on the search performed using keywords relevant to the study. The result is 70 articles, as shown in Figure 3.

3.6 Quality Assessment

It is crucial to conduct a thorough examination of the quality of the selected articles to be included in the final sample. During this stage, the chosen articles were evaluated using seven quality criteria. The quality assessment (QA) criteria used to evaluate the articles are detailed in Table 4.

For each document, a full read was conducted, and the 7 quality criteria were applied using a scale of 1 to 3, where 1 represents "Not good," 2 "Good," and 3 "Very good." The minimum score required for inclusion in the study was 11.5. Of the 70 articles evaluated, all primary studies reached a value equal to or greater than 11.5 on the quality criteria (QA). The results of this quality evaluation are presented in Table 5.

3.7 Data Extraction Strategies

At this stage, after obtaining the final list of articles, the extraction of information necessary to answer all the posed research questions was carried out. The information extracted from each article included the article's title, URL, source, year of publication, country, ISSN, type of publication, publication name, authors, affiliation, quartile, H-index, number of citations, abstract, and keywords. It is important to note that not all articles provided answers to all research questions. The Mendeley Desktop tool was used for managing this data.

3.8 Synthesis of Findings

The information extracted to answer each of the research questions RQ1-RQ5 was tabulated and presented as quantitative data, which was used to develop a statistical comparison between the different findings for each research question. These developed statistics helped to discover certain research patterns as well as research directions that have been undertaken over the last seven years.

Table 4. Quality Assessment Criteria

QA	Criteria
QA1	Does the article focus on theoretical research?
QA2	Are the sources of the data collection methods cited?
QA3	Does the researcher have training in engineering and postgraduate studies?
QA4	Is the research objective explicitly defined?
QA5	Is the full version of the article available?
QA6	Does the article describe the environment of the conducted research?
QA7	Are the experimental findings communicated transparently?

4 Results and Discussion

4.1 General Overview of the Studies

The study selection process resulted in 70 studies chosen for data extraction and analysis. Figure 4 shows the distribution of the published studies and their trend from 2016 to 2022.

Regarding the trend: With the estimated STM (structural topic modeling) parameters, the proportion of each topic is calculated:

$$\mathrm{Pk} = \frac{\sum_{\mathrm{d}} \theta_{\mathrm{d,k}}}{\mathrm{D}}, \tag{1}$$

where *Pk* is the k-th thematic proportion, $\theta_{d,k}$ is the k-th thematic proportion in the d-th document, and D is the total number of selected documents.

$$\mathrm{S} = \sum_{\mathrm{i=1}}^{\mathrm{n-1}} \sum_{\mathrm{j=i+1}}^{\mathrm{n}} \mathrm{sign}\left(\mathrm{X_j} - \mathrm{X_i}\right), \tag{2}$$

$$\mathrm{sign}\left(\mathrm{X_j} - \mathrm{X_i}\right) = \begin{cases} -1 \text{ if } (\mathrm{X_j} - \mathrm{X_i}) < 0 \\ 0 \text{ if } (\mathrm{X_j} - \mathrm{X_i}) = 0 \\ 1 \text{ if } (\mathrm{X_j} - \mathrm{X_i}) > 0 \end{cases}. \tag{3}$$

Given a time series Xi = x_1, x_2, …, x_n, the test statistic S is determined by:

n represents the number of data points, x_i and x_j are the values at times i and j (j>i), respectively, and sign (x_i y x_j) is the sign function S is a normal distribution with E(S) and variance V(S) expressed as:

Table 5. Quality Evaluation Results

Article	Type	QA1	QA2	QA3	QA4	QA5	QA6	QA7	Score
[1]	Journal	1	3	1	2	2	2	1	12
[2]	Journal	3	2	3	2	3	1	2	16
[3]	Journal	1	1	1	1	2	3	3	12
[4]	Journal	3	3	1	2	2	1	1	13
[5]	Journal	3	2	2	2	1	2	1	13
[6]	Journal	1	2	1	3	2	2	1	12
[7]	Journal	2	3	2	3	3	3	3	19
[8]	Journal	2	3	3	1	2	3	3	17
[9]	Journal	3	1	2	1	2	2	3	14
[10]	Journal	3	3	3	3	3	3	3	21
[11]	Journal	3	1	3	1	1	1	3	13
[12]	Journal	3	1	3	3	3	3	1	17
[13]	Journal	2	2	2	2	2	2	1	13
[14]	Journal	2	3	2	2	2	2	1	14
[15]	Journal	1	2	3	3	1	1	1	12
[16]	Journal	3	3	3	1	2	2	3	17
[17]	Journal	3	2	1	1	2	2	2	13
[18]	Journal	2	2	3	2	3	1	1	14
[19]	Journal	2	2	2	1	1	2	3	13
[20]	Journal	3	1	3	3	3	2	2	17
[21]	Journal	1	1	2	2	2	3	1	12
[22]	Journal	1	2	3	1	3	1	2	13
[23]	Journal	1	3	2	1	1	2	2	12
[24]	Journal	2	2	3	1	2	1	1	12
[25]	Journal	3	2	1	3	2	3	3	17
[26]	Journal	1	3	2	1	1	1	3	12
[27]	Journal	1	3	1	3	2	1	2	13
[28]	Journal	3	3	1	2	2	1	1	13
[29]	Journal	2	3	2	3	3	3	1	17
[30]	Journal	2	2	3	2	2	1	1	13
[31]	Journal	3	3	2	3	2	1	3	17
[32]	Journal	3	1	1	1	3	2	2	13
[33]	Journal	1	2	2	2	1	3	1	12
[34]	Journal	1	1	2	3	2	1	3	13
[35]	Journal	2	1	2	1	3	3	3	15
[36]	Journal	3	2	1	3	2	1	1	13
[37]	Journal	2	1	1	3	2	3	2	14
[38]	Journal	1	3	2	2	3	1	3	15
[39]	Journal	3	3	1	1	2	1	3	14
[40]	Journal	3	3	2	1	2	1	2	14
[41]	Journal	3	2	1	1	2	3	1	13
[42]	Journal	2	2	3	2	2	3	3	17
[43]	Journal	3	3	1	2	1	2	1	13
[44]	Journal	3	3	2	2	3	3	1	17
[45]	Journal	2	1	3	3	2	3	1	15
[46]	Journal	3	1	3	1	2	1	1	12
[47]	Journal	1	3	2	3	2	3	2	16
[48]	Journal	1	2	2	3	3	2	2	15
[49]	Journal	3	2	2	1	2	1	2	13
[50]	Journal	3	2	2	3	3	3	1	17

[51]	Journal	3	1	1	3	3	1	1	13
[52]	Journal	3	2	2	3	1	3	1	15
[53]	Journal	2	1	1	3	3	2	2	14
[54]	Journal	2	3	1	3	2	1	3	15
[55]	Journal	1	2	2	2	1	3	1	12
[56]	Journal	3	3	2	2	2	3	2	17
[57]	Journal	2	3	3	3	2	1	3	17
[58]	Journal	2	3	3	2	3	1	3	17
[59]	Journal	2	2	1	3	3	2	2	15
[60]	Journal	3	3	3	2	1	3	2	17
[61]	Journal	1	1	3	2	3	1	3	14
[62]	Journal	2	2	2	3	3	3	3	18
[63]	Journal	1	3	3	3	3	2	3	18
[64]	Journal	2	1	3	3	2	2	3	16
[65]	Journal	3	3	2	1	2	2	3	16
[66]	Journal	2	2	1	1	2	2	2	12
[67]	Journal	1	3	1	2	1	3	3	14
[68]	Journal	1	1	2	1	3	1	3	12
[69]	Journal	1	3	3	1	2	3	2	15
[70]	Journal	1	1	1	3	2	2	2	12

Fig. 4. Distribution of published papers by year

$$E(S) = 0,$$
$$V(S) = \frac{n(n-1)(2n+5)}{18}. \quad (4)$$

$$Z = \begin{cases} \frac{S-1}{\sqrt{V(S)}} \text{ if } S > 0, \\ 0 \text{ if } S = 0, \\ \frac{S+1}{\sqrt{V(S)}} \text{ if } S < 0. \end{cases} \quad (5)$$

Z is represented by the Equation:

A positive/negative Z reflects an increasing/ decreasing trend.

A polynomial regression is determined within the framework of computer security for IoT devices:

$$y = \beta_0 + \beta_1 x + \beta_2 x^2 + \cdots + \beta_n x^n, \quad (6)$$

where: y is the response variable we want to predict, x is the feature, β_0 is the y-intercept, the other βs, are the coefficients/parameters we would like to find when we train our model on the available x and y values, n is the degree of the polynomial (the higher n, the more complex curves that can be created).

In this equation, the number of coefficients (βs) is determined by the highest power of the feature (that is, the degree of our polynomial; β_0 is not considered because it is the interception).

Kendall's trend analysis shows a significant increase in the number of articles published annually on cybersecurity, with particularly notable growth starting from 2020. The p-value (0.007) confirms that the upward trend is statistically significant, while the high coefficient of determination R2 (0.97) indicates that the cubic regression model reliably explains the variability in the publication data over time. Furthermore, applying the equation for the year 2023 results in a similar quantity to 2022, that is, approximately 23 articles.

The increasing trend in the number of articles published per year is reflected in the years 2016 – 2020. In a study related to the research topic, Li [80] shows the same trend but in the years 2010 – 2016. Additionally, for Abdullahi [71] and Fazli [82], it is observed that the number of studies has significantly increased over the years, meaning that the field of cybersecurity and IoT is gaining popularity and receiving more and more attention from various scholars.

These results underscore a growing focus and urgency in cybersecurity research, possibly driven by the expansion of IoT and the emergence of more sophisticated security threats. The statistical confirmation of this trend can motivate the allocation of more resources and research efforts in the area, reflecting the importance of cybersecurity in the current scientific and technological agenda.

Table 6. Number of papers by continent and range of H- index

H-index Continent	≤ 20	≥ 21 ≤ 50	≥ 51 ≤ 80	≥ 81	Total
Asia	2	7	2	46	57
Europe	4	8	3	22	37
America	2	4	1	15	22
Oceania		3		7	10
Africa		1	2	4	7
Total	8	23	8	94	133

In Table 6, the number of articles by continent and according to the range of the journal's H-index in which they were published is detailed.

The Asian continent has the highest number of papers, and each of its documents is published in journals with a high H-index, meaning they are considered the most productive and highest impact due to the number of times they have been cited.

In the study by Rejeb [86], it is mentioned that the journal's impact factor is measured from data collected in WoS, which indicates the scientific quality of academic journals. This author mentions that the most relevant journals in IoT research are those with a high h-index.

For Raimundo [84], the h-index was used to determine the productivity and impact of published works, based on the highest 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. The citations of all scientific articles from 2014 to 2021 were also analyzed, with a total of 568 citations.

The h-index is an indicator to measure the professional quality of the authors, based on the number of citations their articles have recorded, the higher this index, the more we can assure that the article is highly referenced by other research. Based on the results, the Asian continent is the place where it is recommended to search for documents for future research since the papers developed in the countries of this continent are highly cited.

4.2 Responses to Research Questions

Below are the responses to the research questions posed in the study. These responses are based on the data obtained and analyzed during the

Table 7. Criteria for assessing cybersecurity

Criteria	Reference	Qty. (%)
Availability	[2][5][6][8][10][11][17][18][23][26] [28][29][31][37][39][40][41][42][43] [44][45][46] [47][48][50][52][53][55] [56][57][58][59][64][65][66][67] [69][70]	**38 (54.2)**
Integrity	[2][3][6][9][15][23][29][35][37][39] [44][45][46][48][49][51][52][56] [58][61][67][70]	**22 (31.4)**
Confidentiality	[2][5][6][14][16][18][23][26] [28][29] [35][39][40][41][43][44][45] [46][47] [48][51][52] [55][56][57][58] [59][62] [64] [65][67][69][70]	**33 (47.1)**
Authentication	[6][10][11][12][14][15][16][18] [23][26] [28][29][30][34][39][40] [41][44][45][46][48] [51][52][55] [56][58][59][60][62][64] [65][68][69]	**33 (47.1)**

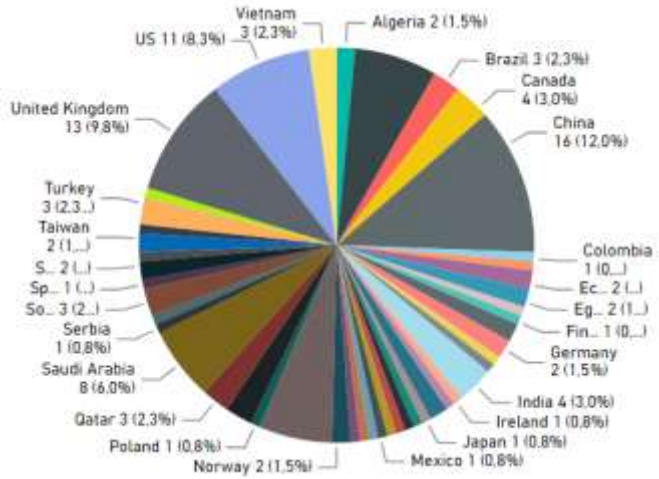

Fig. 5. Number of articles by country

systematic review. Additionally, comments on the findings, discussions on the implications of these results, and suggestions for future research are included.

Principio del formulario

RQ1: What are the criteria for measuring the effectiveness of Cybersecurity?

Table 7 presents the criteria used to evaluate the effectiveness of cybersecurity. During the research, four key criteria were identified to measure the performance of practices implemented in the protection of systems and confidential information against digital attacks.

These criteria reflect how the robustness of security measures is evaluated in different environments and situations, providing a framework for understanding the efficacy of cybersecurity strategies in practice. Availability is considered the most crucial criterion, reflected in 54.2% of the references, indicating a high priority in keeping services accessible and operational.

Confidentiality and authentication criteria also show significant importance, both cited in 47.1% of cases, emphasizing the need to protect information against unauthorized access and to effectively verify the identity of users. Integrity, at 31.4%, although less cited, remains a vital aspect to ensure data accuracy and non-alteration.

The aspects of security that are most breached is an issue that must be considered. Zagi [89], in his research work, carried out the grouping of articles in which reference is made to the aspects

Fig. 6. Heat map of the number of articles by country

Table 8. Number of research studies by journal quartile levels

Publication Type	SQ	Q1	Q2	Q3	Total
Journal	1	47	20	2	70
Total	1	47	20	2	70

of integrity, availability, confidentiality, authorization, and authentication, which as a result, are observed to be the most violated security aspects, therefore these can be considered as criteria to confirm that a system or device is protected. For Rajmohan [85] and Tange [87], the security concern covered in the primary studies is also the aforementioned criteria, adding to these privacy and resilience.

These findings suggest that cybersecurity strategies should focus on developing and reinforcing measures that primarily ensure availability without compromising the integrity, confidentiality, and authentication of data and users. This balance is essential for effective protection against the growing cyber challenges in digital environments.

RQ2: Which nations lead in generating research on Cybersecurity applied to attacks on IoT devices?

Figure 5 details the volume and percentage of scientific publications by country in the field of cybersecurity for IoT devices.

The chart shows that China (12%), the United Kingdom (9.8%), and the United States (8.3%) lead in scientific production in IoT cybersecurity, reflecting their commitment and investment in this sector. The significant presence of countries like Brazil and Germany indicates global interest and a diversified contribution to research.

Figure 6 provides a geographical representation of research productivity by country, using a map chart for a visual interpretation of the distribution.

Upon examining the map, it is clearly noticeable that China, the United States, the United Kingdom, and Australia are countries with a favorable pattern and trend in the production of published articles in this field.

China produces a large part of the studies on cybersecurity challenges in the IoT sphere. According to Jabbar [77], most of the published research papers come from Chinese institutions, with the United States holding second place, and these countries remain in the top 3 for the most articles published.

For Chipa [74], the United States has the greatest contribution of articles related to the topic of this study. This is a prime example that due to advanced technology in first-world countries and thus the simultaneous growth of cybercrime, there is a noticeable appeal from researchers on the study of security in IoT.

This distribution suggests opportunities to encourage research growth in nations with lower production (red) and to strengthen international collaborations. The results could motivate policies and funding directed at increasing research in countries with growth potential (orange and red).

RQ3: In which quartiles are the journals that disseminate research on the influence of Cybersecurity in mitigating attacks on IoT devices classified?

Table 8 breaks down the quartile (Q) levels of the journals in which the most research articles have been published.

The majority of IoT cybersecurity research is published in first quartile (Q1) journals, underscoring the high quality and relevance of the field.

The also notable presence in the second quartile (Q2) suggests broad academic acceptance. The less frequent occurrence in third quartile (Q3) and unranked (SQ) journals indicates a focus on less prestigious publications.

The total number of research studies was obtained from a single type of publication. Journals, which hold a high degree of relevance in their field, have been taken as the sole type of publication. Nifakos [83], for his study, considered both conferences and journal articles, with the latter accounting for a participation rate of 91.43%.

This is evidence that journal articles are highly sought after by researchers addressing the review topic. According to Raimundo [84], most cybersecurity articles in IoT are situated in the best quartile index, Q1. In Tange [87]'s study, the relevant articles were obtained using a set of criteria, which resulted in 92% at the highest quartile level and the difference belonging to Q2.

This pattern highlights the significance of IoT cybersecurity in the scientific community and can influence the perception of research in this field. The predominance of publications in high quartile journals can increase the visibility of the topic and attract more future research and funding.

Figure 7 displays a Sankey diagram that represents the number of articles by journal quartile, shown on the left side, and by citation range, displayed on the right side. The bands in shades of gray crossing the graph indicate the number of articles corresponding to each quartile.

The significant volume of articles in Q1 journals, especially those cited more than 15 times, underscores the relevance and impact of cybersecurity research for IoT. The presence in Q2 and Q3, though less prominent, complements the research perspective in the academic spectrum. The correlation between high quartiles and a greater number of citations emphasizes the perceived quality and influence of these works.

In line with the above, the expressed information is relevant to assess the quality of published studies and the importance of publishing in high-impact journals. According to Gomes [88], since many articles were recently published when the search in the information sources was conducted, the studies had no or only a few citations (from 1 to 6).

Only a few articles had more than 6 citations, suggesting that most of the articles have not generated significant attention in the scientific community. For Zagi [89], most Q1 journals were published and matched their desired criteria, allowing to ensure the quality, feasibility, and scientific rigor of their study. Clim [75]'s study found that the average number of citations per article was 106, considering that 80 articles from scientific journals were included.

This implies that cybersecurity in IoT is a research area with highly valued and recognized outcomes. The concentration in high-quality journals suggests that the findings are considered robust and reliable, which is vital to influence practice and policy in security for emerging technologies.

RQ4: How are publications that share similar conclusions in studies of Cybersecurity and its impact on IoT device attacks grouped?

Figure 8 displays a scatter plot that identifies clusters where research shares similarities in their conclusions, grouped by colors to differentiate each cluster.

In the figure, four clusters are enumerated from 1 to 4, each presenting certain characteristics, primarily the number of articles in the clusters with similar conclusions. Cluster 1 includes 18 articles, the second cluster 13, the third 14, and the last cluster 25. This grouping contains some peculiarities; articles [23, 58, 50, 22] show a high similarity in their conclusions.

The comparison in this research question was not conducted because, among the fifteen systematic literature reviews of the related works available, no relationship was found with the use of clusters in the research concerning similarity in their conclusions. Therefore, this result is the first to be conducted, and it is hoped that they can be used for future research.

The presence of different clusters underscores the diversity and richness of approaches in IoT cybersecurity research, which is crucial for the comprehensive development of the field. This variability also suggests the possibility of exploring interdisciplinary synergies and the importance of promoting dialogue among various research lines.

RQ5: Which countries show frequent collaboration in research related to Cybersecurity and attacks on IoT devices?

Figure 9 illustrates a network diagram that visualizes collaborations between countries in creating research articles, indicating the interactions and the magnitude of collaboration among various nations.

Thicker connections, especially between the United Kingdom, China, and Pakistan, indicate a high level of collaboration in IoT cybersecurity. The presence of links with countries such as Saudi Arabia and Australia demonstrates a global scope of cooperation. The network also reveals less frequent but significant collaborations with countries like Australia and Vietnam.

Joint participation with other researchers from different countries in research activities is an essential trait in Science, being common in many disciplines. Bello [73] mentions in his review that the United States, China, South Korea, Malaysia, and Russia made significant contributions to research in this field by collaborating with various countries worldwide in the years 2018 - 2020. However, from 2020 onwards, the countries that have emerged as new hubs focused on

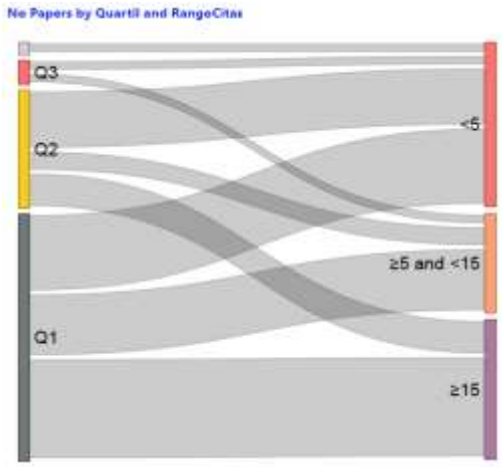

Fig. 7. Number of articles by quartile and citation range

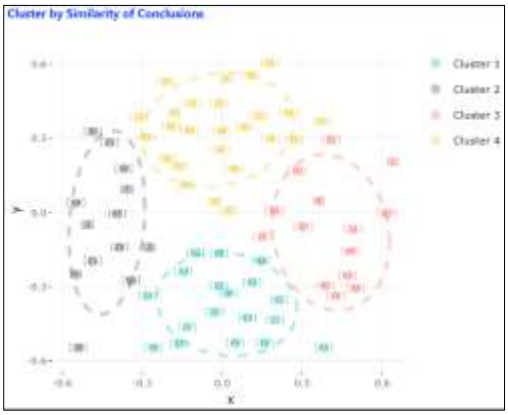

Fig. 8. Cluster by similarity of conclusions

cybersecurity issues and their applications are India, Taiwan, and Denmark.

These trends highlight the importance of international alliances in advancing IoT cybersecurity, which can lead to richer knowledge exchange and innovation. The connections underline the opportunity for countries with emerging collaborations to strengthen their research capabilities through strategic partnerships.

5 Conclusions and Future Research

The rise of the Internet of Things (IoT) has been fundamental for social and global advancement. Devices involved in our daily interactions are

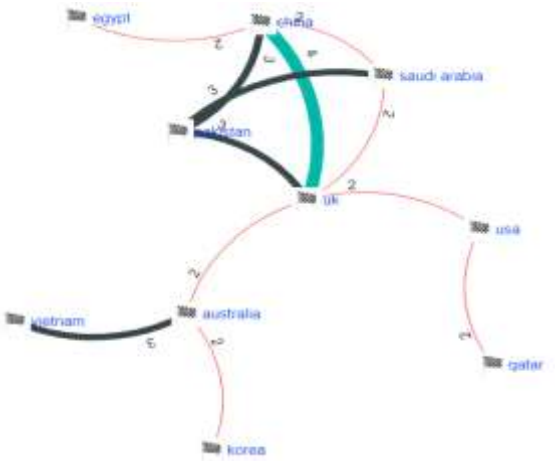

Fig. 9. Bibliometric network by country

evolving into internet-connected objects, increasing their utility in homes and industries. IoT devices have positively revolutionized business and domestic processes, from security cameras to networked machinery and analytical platforms for processing operational data. Cybersecurity is crucial in protecting these devices, safeguarding the integrity, confidentiality, availability, and authentication of information systems—indicators of an efficient security system.

Good practices have been identified to mitigate risks and prevent alterations or attacks that compromise both the information and the functionality of IoT devices.

This systematic review has demonstrated that China, the United Kingdom, and the United States lead in research productivity on IoT. Additionally, the significant collaboration in research between the Asian and North American countries is highlighted, with a special mention to Pakistan for its notable amount of cooperation.

Publications in high-quartile journals have been fundamental in the selection of articles, integrating their total influence in the references of this study.

The systematic review, thanks to a rigorous methodology and well-formulated research questions, has provided valuable knowledge.

On the other hand, it is important to recognize that the search in the information sources was delimited by the specific terms of the research topic. This research serves as a guide for future investigations seeking to delve deeper into issues of Cybersecurity and Cyber Attacks on IoT Devices, contributing to the understanding and continuous enrichment of this critical field.

References

1. **Akbarzadeh, B. A., Katsikas, S. (2022).** Unified IT&OT modeling for cybersecurity analysis of cyber-physical systems. IEEE Open Journal of the Industrial Electronics Society, Vol. 3, pp. 318–328. DOI: 10.1109/OJIES.2022.3178834.
2. **Majumder, A. J. A., Veilleux, C. B., Miller, J. D. (2020).** A cyber-physical system to detect IoT security threats of a smart home heterogeneous wireless sensor node. IEEE Access, Vol. 8, pp. 205989–206002. DOI: 10.1109/ACCESS.2020.3037032.
3. **Aldaej, A., Ahanger, T. A., Atiquzzaman, M., Ullah, I., Yousufudin, M. (2022).** Smart cybersecurity framework for IoT-empowered drones: Machine learning perspective. Sensors, Vol. 22, No. 7, pp. 2630. DOI: 10.3390/s22072630.
4. **Alharbi, S., Attiah, A., Alghazzawi, D. (2022).** Integrating blockchain with artificial intelligence to secure IoT networks: Future trends. Sustainability, Vol. 14, No. 23, pp. 16002. DOI: 10.3390/su142316002.
5. **Althobaiti, O. S., Dohler, M. (2020).** Cybersecurity challenges associated with the internet of things in a post-quantum world. IEEE Access, Vol. 8, pp. 157356–157381. DOI: 10.1109/ACCESS.2020.3019345.
6. **Althobaiti, O. S., Dohler, M. (2021).** Quantum-resistant cryptography for the internet of things based on location-based lattices. IEEE Access, Vol. 9, pp. 133185–133203. DOI: 10.1109/ACCESS.2021.3115087.
7. **Andrade, R., Ortiz-Garcés, I., Tintin, X., Llumiquinga, G. (2022).** Factors of risk analysis for IoT systems. Risks, Vol. 10, No. 8, pp. 162. DOI: 10.3390/risks10080162.
8. **Attota, D. C., Mothukuri, V., Parizi, R. M., Pouriyeh, S. (2021).** An ensemble multi-view federated learning intrusion detection for IoT. IEEE Access, Vol. 9, pp. 117734–117745. DOI: 10.1109/ACCESS.2021.3107337.
9. **Banaamah, A. M., Ahmad, I. (2022).** Intrusion detection in IoT using deep learning. Sensors, Vol. 22, No. 21, pp. 8417. DOI: 10.3390/s22218417.
10. **Bravos, G., Cabrera, A. J., Correa, C., Danilović, D., Evangeliou, N., Ezov, G., Vukobratovic, D. (2022).** Cybersecurity for industrial internet of things:

architecture, models and lessons learned. IEEE Access, Vol. 10, pp. 124747–124765. DOI: 10.1109/ACCESS.2022.3225074.

11. **Cardenas, D. J. S., Hahn, A., Liu, C. C. (2020).** Assessing Cyber-physical risks of IoT-based energy devices in grid operations. IEEE Access, Vol. 8, pp. 61161–61173. DOI: 10.1109/ACCESS.2020.2983313.
12. **Cvitic, I., Perakovic, D., Gupta, B. B., Raymond-Choo, K. K. (2022).** Boosting-based DDoS detection in internet of things systems. IEEE Internet of Things Journal, Vol. 9, No. 3, pp. 2109–2123. DOI: 10.1109/JIOT.2021.3090909.
13. **Dhirani, L. L., Armstrong, E., Newe, T. (2021).** Industrial IoT, cyber threats, and standards landscape: Evaluation and roadmap. Sensors, Vol. 21, No. 11, pp. 3901. DOI: 10.3390/s21113901.
14. **Diro, A. A., Chilamkurti, N., Nam, Y. (2018).** Analysis of lightweight encryption scheme for fog-to-things communication. IEEE Access, Vol. 6, pp. 26820–26830. DOI: 10.1109/ACCESS.2018.2822822.
15. **Diro, A., Reda, H., Chilamkurti, N., Mahmood, A., Zaman, N., Nam, Y. (2020).** Lightweight authenticated-encryption scheme for internet of things based on publish-subscribe communication. IEEE Access, Vol. 8, pp. 60539–60551. DOI: 10.1109/ACCESS.2020.2983117.
16. **Erendor, M. E., Yildirim, M. (2022).** Cybersecurity awareness in online education: A case study analysis. IEEE Access, Vol. 10, pp. 52319–52335. DOI: 10.1109/ACCESS.2022.3171829.
17. **Fang, W., Xu, M., Zhu, C., Han, W., Zhang, W., Rodrigues, J. J. (2019).** FETMS: Fast and efficient trust management scheme for information-centric networking in internet of things. IEEE access, Vol. 7, pp. 13476–13485. DOI: 10.1109/ACCESS.2019.2892712.
18. **Fatani, A., Abd-Elaziz, M., Dahou, A., Al-Qaness, M. A., Lu, S. (2021).** IoT intrusion detection system using deep learning and enhanced transient search optimization. IEEE Access, Vol. 9, pp. 123448–123464. DOI: 10.1109/ACCESS.2021.3109081.
19. **Fatima, H., Khan, H. U., Akbar, S. (2021).** Home automation and RFID-based internet of things security: challenges and issues. Security and Communication Networks, 2021, pp. 1–21. DOI: 10.1155/2021/1723535.
20. **Ferrag, M. A., Friha, O., Hamouda, D., Maglaras, L., Janicke, H. (2022).** Edge-IIoTset: a new comprehensive realistic cyber security dataset of IoT and IIoT applications for centralized and federated learning. IEEE Access, Vol. 10, pp. 40281–40306. DOI: 10.1109/ACCESS.2022.3165809.
21. **Fu, Y., Yan, Z., Cao, J., Koné, O., Cao, X. (2017).** An automata based intrusion detection method for internet of things. Mobile Information Systems, Vol. 2017, No. 1, pp. 1750637**.** DOI: 10.1155/2017/1750637.
22. **Gavel, S., Raghuvanshi, A. S., Tiwari, S. (2021).** Distributed intrusion detection scheme using dual-axis dimensionality reduction for internet of things (IoT). Journal of Supercomputing, Vol. 77, No. 9, pp. 10488–10511. DOI: 10.1007/s11227-021-03697-5.
23. **Goworko, M., Wytrębowicz, J. (2021).** A secure communication system for constrained IoT devices—experiences and recommendations. Sensors, Vol. 21, No. 20, pp. 6906. DOI: 10.3390/s21206906.
24. **Huma, Z. E., Latif, S., Ahmad, J., Idrees, Z., Ibrar, A., Zou, Z., Baothman, F. (2021).** A hybrid deep random neural network for cyberattack detection in the industrial internet of things. IEEE access, Vol. 9, pp. 55595–55605. DOI: 10.1109/ACCESS.2021.3071766.
25. **Jafar, M. T., Al-Fawa'reh, M., Barhoush, M., Alshira'H, M. H. (2022).** Enhanced analysis approach to detect phishing attacks during COVID-19 crisis. Cybernetics and Information Technologies, Vol. 22, No. 1, pp. 60–76. DOI: 10.2478/cait-2022- 0004.
26. **Kandasamy, K., Srinivas, S., Achuthan, K., Rangan, V. P. (2020).** IoT cyber risk: a holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. EURASIP Journal on Information Security, Vol. 2020, No. 1, pp. 8. DOI: 10.1186/s13635-020-00111-0.
27. **Kasper, A., Osula, A. M., Molnár, A. (2021).** EU cybersecurity and cyber diplomacy. IDP Revista de Internet, Derecho y Política, Vol. 34, No. 34, pp. 1–15. DOI: 10.7238/idp.v0i34.387469.
28. **Khan, I. U., Aslam, N., AlShedayed, R., AlFrayan, D., AlEssa, R., AlShuail, N. A., Al-Safwan, A. (2022).** A proactive attack detection for heating, ventilation, and air conditioning (HVAC) system using explainable extreme gradient boosting model (XGBoost). Sensors, Vol. 22, No. 23, pp. 9235. DOI: 10.3390/s22239235.
29. **Khurshid, A., Alsaaidi, R., Aslam, M., Raza, S. (2022).** EU Cybersecurity Act and IoT certification: landscape, perspective and a proposed template scheme. IEEE Access, Vol. 10, pp. 129932–129948. DOI: 10.1109/ACCESS.2022.3225973.
30. **Latif, S., e-Huma, Z., Jamal, S. S., Ahmed, F., Ahmad, J., Zahid, A., Abbasi, Q. H. (2021).** Intrusion detection framework for the internet of

things using a dense random neural network. IEEE Transactions on Industrial Informatics, Vol. 18, No. 9, pp. 6435–6444. DOI: 10.1109/TII.2021.3130248.

31. **Latif, S., Zou, Z., Idrees, Z., Ahmad, J. (2020).** A novel attack detection scheme for the industrial internet of things using a lightweight random neural network. IEEE Access, Vol. 8, pp. 89337–89350. DOI: 10.1109/ACCESS.2020.2994079.
32. **Le, T. D., Ge, M., Anwar, A., Loke, S. W., Beuran, R., Doss, R., Tan, Y. (2022).** Gridattackanalyzer: A cyber attack analysis framework for smart grids. Sensors, Vol. 22, No. 13, pp. 4795**.** DOI: 10.3390/s22134795.
33. **Lei, W., Wen, H., Hou, W., Xu, X. (2021).** New security state awareness model for IoT devices with edge intelligence. IEEE Access, Vol. 9, pp. 69756–69765. DOI: 10.1109/ACCESS.2021.3075220.
34. **Li, C. T., Wu, T. Y., Chen, C. L., Lee, C. C., Chen, C. M. (2017**). An efficient user authentication and user anonymity scheme with provably security for IoT-based medical care system. Sensors, Vol. 17, No. 7, pp. 1482. DOI: 10.3390/s17071482.
35. **Lin, H., Bergmann, N. (2016).** IoT Privacy and security challenges for smart home environments. Information, Vol. 7, No. 3, pp. 44. DOI: 10.3390/info7030044.
36. **Lysenko, S., Bobrovnikova, K., Kharchenko, V., Savenko, O. (2022).** IoT multi-vector cyberattack detection based on machine learning algorithms: Traffic features analysis, experiments, and efficiency. Algorithms, Vol. 15, No. 7, pp. 239. DOI: 10.3390/a15070239.
37. **Mendez-Mena, D., Papapanagiotou, I., Yang, B. (2018).** Internet of things: survey on security. Information security journal: A global perspective, Vol. 27, No. 3, pp. 162–182. DOI: 10.1080/19393555.2018.1458258.
38. **Mercado-Velazquez, A. A., Escamilla-Ambrosio, P. J., Ortiz-Rodriguez, F. (2021).** A moving target defense strategy for internet of things cybersecurity. IEEE Access, Vol. 9, pp. 118406–118418. DOI: 10.1109/ACCESS.2021.3107403
39. **Nespoli, P., Díaz-López, D., Gómez-Mármol, F. (2021).** Cyberprotection in IoT environments: A dynamic rule-based solution to defend smart devices. Journal of Information Security and Applications, Vol. 60, pp. 102878. DOI: 10.1016/j.jisa.2021.102878
40. **Nguyen, T. G., Phan, T. V., Nguyen, B. T., So-In, C., Baig, Z. A., Sanguanpong, S. (2019).** SeArch: A collaborative and intelligent NIDS architecture for SDN-based cloud IoT networks. IEEE Access, Vol. 7, pp. 107678–107694. DOI: 10.1109/ACCESS.2019.2932438.
41. **Okutan, A., Yang, S. J. (2019).** ASSERT: Attack synthesis and separation with entropy redistribution towards predictive cyber defense. Cybersecurity, Vol. 2, No. 1, pp. 15. DOI: 10.1186/s42400-019- 0032-0.
42. **Oriola, O., Adeyemo, A. B., Papadaki, M., Kotzé, E. (2021).** A collaborative approach for national cybersecurity incident management. Information and Computer Security, Vol. 29, No. 3, pp. 457–484. DOI: 10.1108/ICS-02-2020-0027.
43. **Ouaissa, M., Ouaissa, M. (2020).** Cyber security issues for IoT based smart grid infrastructure. IOP Conference Series: Materials Science and Engineering, Vol. 937, No. 1, pp. 012001. DOI: 10.1088/1757-899X/937/1/012001.
44. **Pinto, R., Gonçalves, G., Delsing, J., Tovar, E. (2022).** Enabling data-driven anomaly detection by design in cyber-physical production systems. Cybersecurity, Vol. 5, No. 1. DOI: 10.1186/s42400-022-00114-z.
45. **Rahal, B. M., Santos, A., Nogueira, M. (2020).** A distributed architecture for DDoS prediction and bot detection. IEEE Access, Vol. 8, pp. 159756–159772. DOI: 10.1109/ACCESS.2020.3020507.
46. **Raju, A. D., Abualhaol, I. Y., Giagone, R. S., Zhou, Y., Huang, S. (2021).** A survey on cross-architectural IoT malware threat hunting. IEEE Access, Vol. 9, pp. 91686–91709. DOI: 10.1109/ACCESS.2021.3091427.
47. **Rana, M. U., Ellahi, O., Alam, M., Webber, J. L., Mehbodniya, A., Khan, S. (2022).** Offensive security: cyber threat intelligence enrichment with counterintelligence and counterattack. IEEE Access, Vol. 10, pp. 108760–108774. DOI: 10.1109/ACCESS.2022.3213644.
48. **Rawindaran, N., Jayal, A., Prakash, E. (2022).** Exploration of the impact of cybersecurity awareness on small and medium enterprises (SMEs) in wales using intelligent software to combat cybercrime. Computers, Vol. 11, No. 12, pp. 174. DOI: 10.3390/computers11120174.
49. **Ur-Rehman, S., Khaliq, M., Imtiaz, S. I., Rasool, A., Shafiq, M., Javed, A. R., Bashir, A. K. (2021).** DIDDOS: An approach for detection and identification of distributed denial of service (DDoS) cyberattacks using gated recurrent units (GRU). Future Generation Computer Systems, Vol. 118, pp. 453-466**.** DOI: 10.1016/j.future.2021.01.022.
50. **Saeed, A., Ahmadinia, A., Javed, A., Larijani, H. (2016).** Intelligent intrusion detection in low-power

IoTs. ACM Transactions on Internet Technology, Vol. 16, No. 4, pp. 1–25. DOI: 10.1145/2990499.

51. **Samy, A., Yu, H., Zhang, H. (2020).** Fog-based attack detection framework for internet of things using deep learning. IEEE Access, Vol. 8, pp. 74571–74585. DOI: 10.1109/ACCESS.2020.2988854.
52. **Santos, L., Gonçalves, R., Rabadao, C., Martins, J. (2023).** A flow-based intrusion detection framework for internet of things networks. Cluster Computing, pp. 1–21. DOI: 10.1007/s10586-021-03238-y.
53. **Shafiq, M., Tian, Z., Bashir, A. K., Du, X., Guizani, M. (2020).** IoT malicious traffic identification using wrapper-based feature selection mechanisms. Computer Security, Vol. 94, p. 101863. DOI: 10.1016/j.cose.2020.101863.
54. **Shalaginov, A., Azad, M. A. (2021).** Securing resource-constrained IoT nodes: Towards intelligent microcontroller-based attack detection in distributed smart applications. Future Internet, Vol. 13, No. 11, p. 272. DOI: 10.3390/fi13110272.
55. **Shin, Y., Lee, J., Kim, M. (2018).** Preventing state-led cyberattacks using the bright internet and internet peace principles. Journal of the Association for Information Systems, Vol. 19, No. 3, pp. 152–181. DOI: 10.17705/1jais.00488.
56. **Sohal, A. S., Sandhu, R., Sood, S. K., Chang, V. (2018).** A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments. Computer Security, Vol. 74, pp. 340–354. DOI: 10.1016/j.cose.2017.08.016.
57. **Song, L., Ju, X., Zhu, Z., Li, M. (2021).** An access control model for the internet of things based on zero-knowledge token and blockchain. EURASIP Journal on Wireless Communications and Networking, Vol. 2021, No. 1, pp. 105. DOI: 10.1186/s13638-021- 01986-4.
58. **Süren, E., Heiding, F., Olegård, J., Lagerström, R. (2022).** PatrIoT: practical and agile threat research for IoT. International Journal of Information Security. Vol. 22, pp. 213–233. DOI: 10.1007/s10207-022-00633-3.
59. **Süzen, A. A. (2020).** A risk-assessment of cyber attacks and defense strategies in industry 4.0 ecosystem. International Journal of Computer Network and Information Security, Vol. 12, No. 1, pp. 1–12. DOI: 10.5815/ijcnis.2020.01.01.
60. **Taheri, S., Bagirov, A. M., Gondal, I., Brown, S. (2020).** Cyberattack triage using incremental clustering for intrusion detection systems. International Journal of Information Security, Vol. 19, No. 5, pp. 597–607. DOI: 10.1007/s10207-019-00478-3.
61. **Ullah, F., Naeem, H., Jabbar, S., Khalid, S., Latif, M. A., Al-Turjman, F., Mostarda, L. (2019).** Cyber security threats detection in internet of things using deep learning approach. IEEE Access, Vol. 7, pp. 124379–124389. DOI: 10.1109/ACCESS.2019.2937347.
62. **Ullah, I., Mahmoud, Q. H. (2022).** Design and development of RNN anomaly detection model for IoT networks. IEEE Access, Vol. 10, pp. 62722–62750. DOI: 10.1109/ACCESS.2022.3176317.
63. **Vamsi, P. R., Kant, K. (2016).** Trust aware data aggregation and intrusion detection system for wireless sensor networks. International Journal of Smart Sensors and Intelligent Systems, Vol. 9, No. 2, pp. 537–562. DOI: 10.21307/ijssis-2017-883.
64. **Villegas-Ch., W., Ortiz-Garces, I., Sánchez-Viteri, S. (2021).** Proposal for an implementation guide for a computer security incident response team on a university campus. Computers, Vol. 10, No. 8, pp. 102. DOI: 10.3390/computers10080102.
65. **Vu, L., Nguyen, Q. U., Nguyen, D. N., Hoang, D. T., Dutkiewicz, E. (2020).** Deep transfer learning for IoT attack detection. IEEE Access, Vol. 8, pp. 107335–107344. DOI: 10.1109/ACCESS.2020.3000476.
66. **Wang, C. (2020).** IoT anomaly detection method in intelligent manufacturing industry based on trusted evaluation. International Journal of Advanced Manufacturing Technology, Vol. 107, No. 3–4, pp. 993–1005. DOI: 10.1007/s00170-019-04274-0.
67. **Wang, Y., Che, T., Zhao, X., Zhou, T., Zhang, K., Hu, X. (2022).** A blockchain-based privacy information security sharing scheme in industrial internet of things. Sensors, Vol. 22, No. 9, pp. 3426. DOI: 10.3390/s22093426.
68. **Wazzan, M., Algazzawi, D., Albeshri, A., Hasan, S., Rabie, O., Asghar, M. Z. (2022).** Cross deep learning method for effectively detecting the propagation of IoT botnet. Sensors, Vol. 22, No. 10, p. 3895. DOI: 10.3390/s22103895.
69. **Xu, Q., Jia, X., Jia, B., Liang, Y. (2022).** IoT-oriented distributed intrusion detection methods using intelligent classification algorithms in spark. Security and Communication Networks, Vol. 2022, pp. 1–11. DOI: 10.1155/2022/2842624.
70. **Zolanvari, M., Teixeira, M. A., Gupta, L., Khan, K. M., Jain, R. (2019).** Machine learning-based network vulnerability analysis of industrial internet of things. IEEE Internet of Things Journal, Vol. 6, No. 4, pp. 6822–6834. DOI: 10.1109/JIOT.2019.2912022.
71. **Abdullahi, M., Baashar, Y., Alhussian, H., Alwadain, A., Aziz, N., Capretz, L. F., Abdulkadir,**

S. J. (2022). Detecting cybersecurity attacks in internet of things using artificial intelligence methods: A systematic literature review. Electronics, Vol. 11, No. 2, p. 198. DOI: 10.3390/electronics11020198.

72. **Andrade, R. O., Yoo, S. G., Tello-Oquendo, L., Ortiz-Garces, I. (2020).** A comprehensive study of the IoT cybersecurity in smart cities. IEEE Access, Vol. 8, pp. 228922–228941. DOI: 10.1109/ACCESS. 2020.3046442.
73. **Bello, A., Jahan, S., Farid, F., Ahamed, F. (2022).** A systemic review of the cybersecurity challenges in australian water infrastructure management. Water, Vol. 15, No. 1, pp. 168. DOI: 10.3390/w15010168.
74. **Chipa, I. H., Gamboa-Cruzado, J., Villacorta, J. R. (2022).** Mobile applications for cybercrime prevention: A comprehensive systematic review. International Journal of Advanced Computer Science and Applications, Vol. 13, No. 10, pp. 73–82. DOI: 10.14569/IJACSA.2022.0131010.
75. **Clim, A., Toma, A., Zota, R. D., Constantinescu, R. (2022).** The need for cybersecurity in industrial revolution and smart cities. Sensors, Vol. 23, No. 1, pp. 120. DOI: 10.3390/s23010120.
76. **El, A., Essaaidi, M., Boulmalf, M., El-Majdoubi, D. (2021).** Systematic literature review of internet of things (IoT) security. Advances in Dynamic Systems and Applications, Vol. 16, No. 2, pp. 1671–1692.
77. **Jabbar, R., Dhib, E., Said, A. B., Krichen, M., Fetais, N., Zaidan, E., Barkaoui, K. (2022).** Blockchain technology for intelligent transportation systems: A systematic literature review. IEEE Access, Vol. 10, pp. 20995–21031. DOI: 10.1109/ ACCESS.2022.3149958
78. **Kitchenham, B., Charters, S. (2007).** Guidelines for performing systematic literature reviews in software engineering. Technical report, Version 2.3 EBSE Tech. Report. https://userpages.uni-koblenz.de/~ laemmel/esecourse/slides/slr.pdf.
79. **Lee, I. (2020).** Internet of things (IoT) cybersecurity: literature review and IoT cyber risk management. Future Internet, Vol. 12, No. 9, pp. 157. DOI: 10.339 0/fi12090157.
80. **Li, G., Ren, L., Fu, Y., Yang, Z., Adetola, V., Wen, J., O'Neill, Z. (2023).** A critical review of cyber-physical security for building automation systems. Annual Reviews in Control, Vol. 55, pp. 237–254. DOI: 10.1016/j.arcontrol.2023.02.004.
81. **Liao, B., Ali, Y., Nazir, S., He, L., Khan, H. U. (2020).** Security analysis of IoT devices by using mobile computing: A systematic literature review. IEEE Access, Vol. 8, pp. 120331–120350. DOI: 10.1109/ACCESS.2020.3006358.
82. **Mohd-Sam, M. F., Feisal-Ismail, A. F. M., Abu-Bakar, K., Ahamat, A., Qureshi, M. I. (2022).** The effectiveness of IoT based wearable devices and potential cybersecurity risks: A systematic literature review from the last decade. International Journal of Online and Biomedical Engineering, Vol. 18, No. 09, pp. 56–73. DOI: 10.3991/ijoe.v18i09.32255.
83. **Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., Bonacina, S. (2021**). Influence of human factors on cyber security within healthcare organisations: A systematic review. Sensors, Vol. 21, No. 15, pp. 5119. DOI: 10.3390/s21155119.
84. **Raimundo, R. J., Rosário, A. T. (2022).** Cybersecurity in the internet of things in industrial management. Applied Sciences, Vol. 12, No. 3, p. 1598. DOI: 10.3390/app12031598.
85. **Rajmohan, T., Nguyen, P. H., Ferry, N. (2022).** A decade of research on patterns and architectures for IoT security. Cybersecurity, Vol. 5, No. 1, p. 2. DOI: 10.1186/s42400-021-00104-7.
86. **Rejeb, A., Rejeb, K., Zailani, S. H. M., Abdollahi, A. (2022).** Knowledge diffusion of the internet of things (IoT): A main path analysis. wireless personal communications, Vol. 126, No. 2, pp. 1177–1207. DOI: 10.1007/s11277-022-09787-8.
87. **Tange, K., De-Donno, M., Fafoutis, X., Dragoni, N. (2020).** A systematic survey of industrial internet of things security: Requirements and fog computing opportunities. IEEE Communications Surveys & Tutorials, Vol. 22, No. 4, pp. 2489–2520. DOI: 10.1109/COMST.2020.3011208.
88. **Gomes-Valadares, D. C., Will, N. C., Caminha, J., Barbosa-Perkusich, M., Perkusich, A., Acosta-Gorgonio, K. (2021).** Systematic literature review on the use of trusted execution environments to protect cloud/fog-based internet of things applications. IEEE Access, Vol. 9, pp. 80953–80969. DOI: 10.1109/ ACCESS.2021.3085524.
89. **Zagi, L. M., Aziz, B. (2020).** Privacy attack on IoT: a systematic literature review. 2020 International Conference on ICT for Smart Society (ICISS), pp. 1–8. DOI: 10.1109/ICISS50791.2020.9307568.

Article received on 04/06/2024; accepted on 01/07/2024.
**Corresponding author is Mario Padilla-Gomez.*