E-ISSN: 2583-9667
Indexed Journal
Peer Reviewed Journal
https://multiresearchjournal.theviews.in

Received: 01-05-2023
Accepted: 03-07-2023

INTERNATIONAL JOURNAL OF ADVANCE RESEARCH IN MULTIDISCIPLINARY

Volume 1; Issue 1; 2023; Page No. 836-841

Cyber security in the age of internet of things

[1]P Vivekanand and [2]Dr. Kamal Kumar Srivastava

[1]Research Scholar, Sunrise University, Alwar, Rajasthan, India
[2]Professor, Sunrise University, Alwar, Rajasthan, India

DOI: https://doi.org/10.5281/zenodo.14246392

Corresponding Author: P Vivekanand

Abstract

Intelligent objects in the IoT are made up of a wide variety of sensors, networks, electrical devices, and process technologies that all work together to offer consumers with efficient and insightful services. The concept of a "smart city," in which residents enjoy improved quality of life thanks to cutting-edge infrastructure, has been presented as a means of addressing urban issues. The goal of this article is to present a comprehensive evaluation of IoT technology, with special attention paid to its potential for harm in the areas of privacy and security. Researchers are studying the services provided and the difficulties of IoT to improve the efficacy of Smart Cities. When it comes to ICT, there is still some room for improvement between theory and practice. Security and privacy needs of IoT users have been established to bring attention to the most pressing issues facing this demographic. This IoT privacy and security research makes use of a systematic literature review by searching for relevant publications across a variety of electronic databases and other sources, entering the material into a custom database, and producing summary tables. Collection of studies. As a result, the article provides a concise summary of the most recent developments in IoT privacy and security, draws attention to the most pressing problems, and makes recommendations for further study.

Keywords: IoT, security machine, learning, block chain, threats security

Introduction

Industrial, touristic, and energy sectors are just a few of the many that stand to benefit greatly from the IoT's efforts to merge the virtual and real worlds. As a result, a new set of processes are being driven by a system of interconnected machines and gadgets that are able to communicate and operate together. However, the IoT is vulnerable in the face of numerous security vulnerabilities that may be very difficult to solve because of the complexity of the context and the sheer number of instruments involved, each of which has its own resource limitations. The Internet of Things (IoT) is a network that uses sensors to connect the online and offline worlds. To manage the hardware, software, sensors, and connectivity that enable the interconnection, collection, and exchange of data across a network of IoT devices, home appliances, and vehicles presents a formidable technical challenge. The "smart factory" is the backbone of the Internet of Things since it incorporates human beings, processes, intelligent objects, and technical ecosystems. The Internet of Things extends the concept of internet connection to things that aren't computers, such vehicles and power equipment. The IIoT, cloud computing, big data analytics, and automated manufacturing are all components of the IoT that work together to create low-cost, high-quality goods.

Due to the IoT's widespread adoption across industries, new cyber threats have emerged in areas like as the Internet of Battlefield Things (IoBT) and the Internet of Vehicles (IoV). Since there has been no clear policy direction or comprehension of user values in regards to cybersecurity in terms of the Internet of Things, there has been a recent uptick in anxiety in this area.

Cybersecurity refers to the practice of keeping computer systems, their data, and the means through which they are accessible safe from intrusion. The goal of security is to protect private data from being improperly accessed, changed, or destroyed by other parties. In light of this, society is becoming more susceptible to cyber-attacks, such as denial-of-service assaults by hackers and insiders, that block direct access to devices, etc., owing to the vast number of already existent IoT-based linked gadgets. Cybercrime and cybersecurity tools develop in tandem as

technology becomes ever more integral to our everyday lives; as a result, the whole industrial sector must invest in cybersecurity countermeasures, and new technologies are developing for managing the cybersecurity of the Internet of Things.

In addition, the safety of individuals and governments is adversely impacted by cyber-attacks on smart grids since these critical infrastructure components are especially susceptible and suffer significant consequences. The absence of effective countermeasures, such as cybersecurity specialists, is a rising source of worry. For instance, China is working on new cybersecurity legislation and policy. Moreover, although healthcare is trending because there is so much vital data, cyber protections are often low at hospitals, putting patients' lives and confidence at danger.

There is a vacuum in our understanding of frameworks to handle the complex cybersecurity concerns in the IoT since most existing material focuses on the technical characteristics of IoT cybersecurity. Literature on industrial cyber risk management and Internet of Things (IoT) security technology is reviewed. This article's structure looks like this. We propose many theoretical notions in Section 2 that pertain to IoT cybersecurity. The methodology is described in Section 3. In Section 4, we address the primary applications of cybersecurity in the context of the IoT that have emerged from the literature. In the end, we provide some suggestions for follow-up studies and ramifications.

Literature review

The IoT has revolutionized our daily lives and the ways in which we do business and socialize. The proliferation of Internet-connected gadgets has elevated cybersecurity to the forefront of concerns for individuals, organizations, and governments. This article provides an introduction to cybersecurity in the age of the Internet of Things (IoT), discussing the challenges, threats, and protections unique to IoT infrastructures. Potential risks and threats to IoT security are examined in the research. These include, but are not limited to, the lack of standardization across IoT devices, the difficulty of applying security patches, and the difficulty of upgrading IoT devices. The essay also evaluates the present state of IoT security in light of existing security standards and protocols and discusses the challenges associated with implementing effective security measures. Best practices for protecting IoT devices and networks, the use of blockchain technology, and the significance of encryption and access control are discussed as IoT security measures. The essay concludes with case studies and examples of successful IoT security implementations and provides advice for future directions in IoT security research and development.

M Solihat (2021) [1] The purpose of this research is to ascertain the state of cybersecurity in relation to digital data transit. This research used a qualitative descriptive method known as a literature review. The purpose of this research is to demonstrate that being vigilant when surfing the web keeps users secure. With the use of modern digital tools, we may deduce that the goal of cybersecurity is to protect against cybercrime. The results of this study are meant to serve as a cautionary tale for internet users everywhere.

Muhammad Saad (2018) [2] The Internet has quickly become an indispensable tool. There is a steady rise in the number of Internet-enabled gadgets, and some estimate that there will be 34 billion IoT devices in use by 2020. It has been noted that some manufacturers neglected to integrate basic security, making these devices vulnerable to hacking. Most current devices adhere to standards that are simple to install and suitable for most types of data transmission and storage. various devices have various requirements, hence there is no one universal solution for the Internet of Things. This has led to subsets of IoT devices. Security issues in the IoT are the focus of this research, which begins with a review of the IoT's history, architecture, and industrial uses. Also, categorize and investigate privacy risks, including things like conducting a poll and highlighting the obstacles that need to be solved before the Internet of Things can really take off.

Ricardo Jorge Raimundo (2021) [3] People's everyday lives increasingly take place in the realm of the "smart home," but there are also lucrative potential in "industrial smart cities" and "healthcare" sectors. However, safety concerns have been raised. Although security challenges have grown more costly, especially in Industrial Internet of Things (IIoT) sectors, protecting sensitive data and infrastructure is still a top priority for IoT systems. However, there are significant obstacles to addressing these security concerns in IoT settings: Machine resources are constrained since applications run in decentralized settings like Blockchain, smart things are diverse, and sensors have their limits. In this approach, conventional security measures are inappropriate for IoT infrastructures. The Internet of Things (IoT) and the Industrial Internet of Things (IIoT) have both made cybersecurity a top priority as a means of protecting consumers and businesses from potential harm. There have been advancements in IoT security management thanks to new cybersecurity technology and apps. However, cyber risk solutions for the Internet of Things are not as successful as they might be. Seventy relevant publications were uncovered by a thorough Scopus literature study, and their discussions of the potential and challenges in cybersecurity for IIoT are discussed in this review article. Rather than offering specific technological recommendations for addressing network security issues, it tries to convey the current discussion around the topic of IIoT.

Phillip Williams (2022) [4] The Internet of Things (IoT) has a wealth of opportunities for applications across many areas of society, but it also faces significant obstacles. Concerns about personal data protection are one such obstacle. The security of Internet of Things devices is more easily breached. Security solutions that are compatible with IoT devices and applications are few, turning the "internet of insecure things" into a reality. This is mostly attributable to the limitations of IoT devices in terms of space, power, memory, etc. Implementing the security solutions in the hardware of the IoT device is a potential approach to solving this issue, since it goes beyond the typical or traditional ways. More security holes have opened up in IoT networks because of the prevalence of cutting-edge technologies like machine learning, blockchain, fog/edge/cloud computing, and quantum computing. IoT security risks and mitigation strategies are explored in this article. This poll also details the benefits and drawbacks of integrating cutting-edge technology like machine learning and blockchain into IoT, as well as possible solutions to

these problems. The 4-layer IoT architecture is used as a frame of reference throughout the study to pinpoint security concerns and provide solutions.

Materials and Methods

In this work, the SLR process and the approach are used to develop Internet of Things (IoT) applications for Smart Cities. The three basic components of this study are (1) preparation, (2) investigation, and (3) documentation. All of them are listed in the following figure 1, with detailed descriptions of each procedure.

Step-1 Planning

Throughout this stage, we settled on the review's central topic and carried out the supplementary tasks that elucidated each successive phase. The primary goals of this STR are to learn more about the privacy and security features available in IoT-enabled Smart Cities. As a result, we developed several study questions to examine the ecosystem of this Smarts City.

These are the primary areas of inquiry

RQ-1. What is Security and Privacy IoT in Smart City Environment?
RQ-2. How do to secure the IoT Infrastructure?
RQ-3. What are the major Challenges or Issues using IoT Technology?
RQ-4. How do to make the effective use of IoT in particular area in term of security?

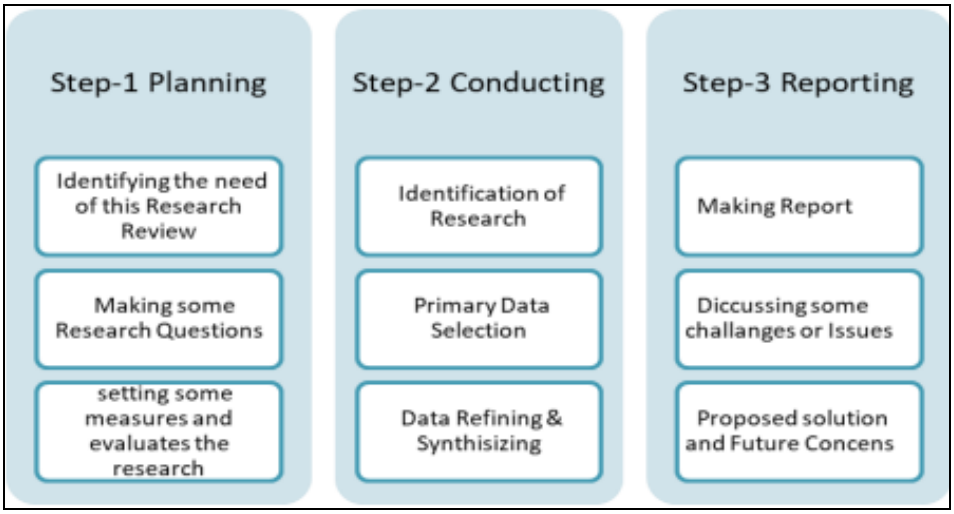

Fig 1: Systematic Literature Review Steps & Activities

Step-2 Conducting Review

This study started with a search of the existing literature using broad Keywords to identify as many relevant publications as possible. Several internet data sets were used to cover a broad range of academic diversity. The following digital libraries and archives were mined for this study: Google Scholar, Springer, IEEE Explorer Access, Research Gates, the ACM Digital Library, and other Web of Science. Considered relevant, these data sets also provide a wide variation of significant impact sizes. Based on the review's examination question, we narrowed our attention on "Security and Privacy of the Internet of Things IoT" and a few associated topics in order to implement the programmed search. Data from scholarly articles were gathered and shown in Fig. 2.

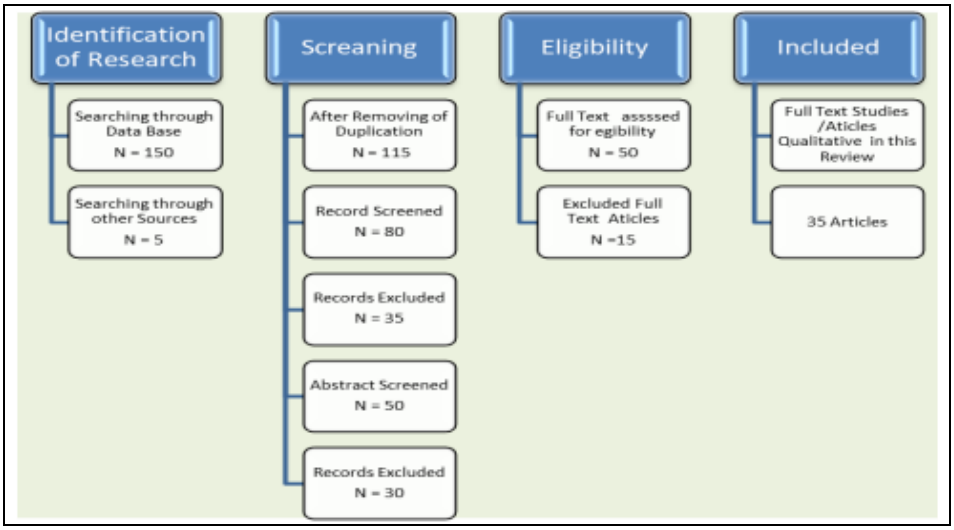

Fig 2: Flow of PRISMA Technique

In this table 1, we provide all of the articles, books, and chapters that were taken into final consideration along with their respective publishers, publication years, and citation references. Out of the thousands of publications in the prestigious online database, 35 were chosen as most pertinent to our investigation.

Table 1: Major Security Issues in IoTs

Sr. No.	Main Data Sources	Publisher Name	Publish Year	Ref. #
1	Google Scholar, Web of Science, Scopus, IEEE Access, Academia, Resarchgate Internet, Websites E-books, books chapters, E-libraries	ACM	2022	[31]
2		AETiC	2020	[7]
3		Elsevier	2020	[13]
4			2018	[18]
5			2022	[20]
6			2022	[23]
7			2018	[24]
8			2021	[28]
9			2018	[32]
10			2020	[33]
11		FCS	2015	[1]
12		Hindawi	2021	[15]
13		ICITSI	2017	[12]
14		IEEE	2017	[2]
15			2017	[6]
16			2014	[10]
17			2016	[11]
18			2022	[17]
19			2022	[21]
20			2023	[26]
21			2017	[29]
22			2016	[8]
23		IJSRCSEIT	2019	[27]
24		IJTRA	2016	[9]
25		Jaypee University of Information Technology	2017	[5]
26		John Wiley & Sons, Ltd.	2014	[14]
27		MDPI	2022	[19]
28		MDPI	2023	[25]
29		MDPI	2023	[34]
30		Routledge	2019	[3]
31		Springer	2014	[4]
32		Springer	2016	[16]
33		Springer	2022	[22]
34		Springer	2022	[30]
35		Springer	2022	[35]

Data from Table 1 is graphically represented in Fig. 3. The names of the publishing houses appear on the horizontal axis, while the publication year appears on the vertical. Selected works from the years 2008-2023 are being analyzed for this project.

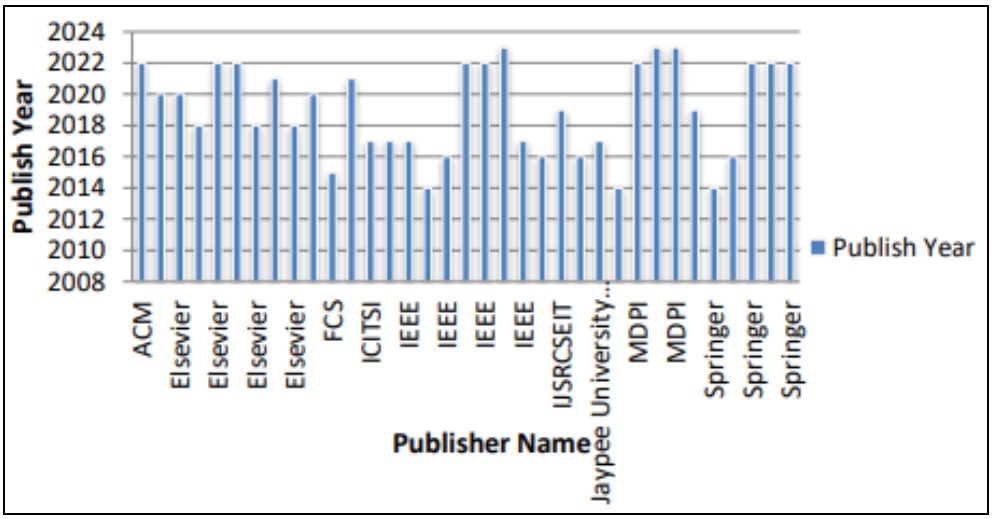

Fig 3: Graph for Publisher and year

Table 2 compiles the authors' summaries of the various publishers' total number of publications under consideration. This evaluation covers 14 unique publishing houses. IEEE and Elsevier both agree that nine is the highest possible number.

Table 2: Summary of inclusion

Sr. No.	Publisher Name	No. Publication
1	ACM	1
2	AETiC	1
3	Elsevier	8
4	FCS	1
5	Hindawi	1
6	ICITSI	1
7	IEEE	9
8	IJSRCSEIT	1
9	IJTRA	1
10	Jaypee University of Information Technology	1
11	John Wiley & Sons, Ltd.	1
12	MDPI	3
13	Routledge	1
14	Springer	5

Data from Table 2 are graphically represented in Fig. 4. On the horizontal axis are the names of the publishers, and on the vertical axis are the totals for the relevant publications. Because IEEE has a greater number, it appears at the top of the graph.

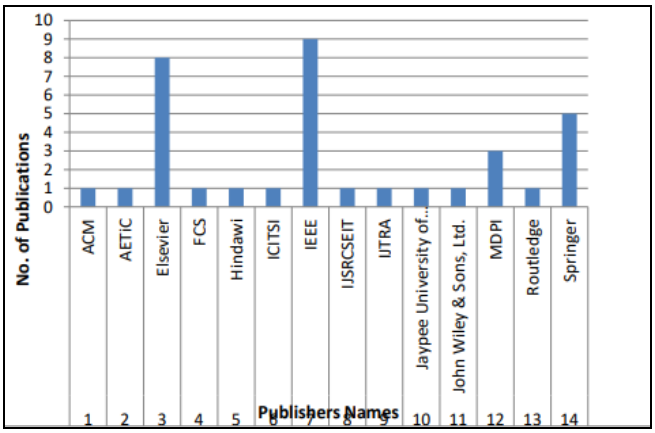

Fig 4: Graph of No. Publication and Publishers

Step-3 Reporting

Thematic analysis, which methodically analyzes areas of security, privacy applications, and services, was used to assess the studies found in the reviews against the backdrop of the stated research topics. In order to address the study questions, it is necessary to identify the obstacles, dangers, and associated problems that must be overcome in order to construct a smart city environment that is both safe and trustworthy. The report is then constructed to respond to the research questions.

Conclusion

The authors provide a list of security and privacy concerns unique to Smart City infrastructure built on the Internet of Things. Systematic literature reviews are used for this purpose. The Internet of Things in modern "Smart Cities" is a must. People want convenient, low-hassle, time- and money-saving, high-quality services sent right to their doors or at least requiring as little of them as possible. The ultimate goal is to make the aforementioned measures even more foolproof. Thus, using ICT, this is possible. A Smart City that makes use of the Internet of Things is able to provide for its residents in a variety of ways. This may be performed effectively by the deployment of security mechanisms. In this analysis, the author discovers many spots where additional effort is required to ensure the reliability of IoT services for human benefit. This study provides a synopsis of key IoT principles, with a focus on the security issues and challenges unique to IoT gadgets. Potential dangers and security holes in the Internet of Things that might discourage its widespread adoption have been identified. We have identified a number of security and privacy problems that the research community needs to overcome in order to establish a dependable and secure platform that can boost public adoption of the technology. There is an immediate need for research institutes in this sector to overcome these security dangers and limitations in IoT based infrastructure so that people may use IoT devices to interact and exchange information internationally with assurance of trust and security.

References

1. Solihat M, Wulansari V. Internet of Things Cyber Security in the Digital Era. IOP Conference Series: Materials Science and Engineering. 2021;1158:012017. DOI: 10.1088/1757-899X/1158/1/012017.
2. Saad M, Soomro T. Cyber Security and Internet of Things. Pakistan J Eng Technol Sci. 2018;7:2084. DOI: 10.22555/pjets.v7i1.2084.
3. Raimundo RJ, Rosário AT. Cybersecurity in the Internet of Things in Industrial Management. Appl Sci. 2021;12:1598. DOI: 10.3390/app12031598.
4. Williams P, Dutta IK, Daoud H, Bayoumi M. A survey on security in internet of things with a focus on the impact of emerging technologies. Internet of Things. 2022;19:100564. DOI: 10.1016/j.iot.2022.100564.
5. Alshboul Y, Bsoul AAR, Zamil MAL, Samarah S. Cybersecurity of smart home systems: Sensor identity protection. J Netw Syst Manag. 2021;29:22.
6. Occa R, Borbon-Galvez Y, Strozzi F. In search of lost security. A systematic literature review on how blockchain can save the IoT revolution. In: Proceedings of the XXV Summer School Francesco Turco, Bergamo, Italy, 11–13 September 2020.
7. Khalid A, Sundararajan A, Hernandez A, Sarwat AI. FACTS approach to address cybersecurity issues in electric vehicle battery systems. Paper presented at: 2019 IEEE Technology and Engineering Management Conference (TEMSCON), Atlanta, GA, USA, 12–14 June 2019.
8. Xie Y, Su X, He Y, Chen X, Cai G, Xu B, *et al.* STM32-based vehicle data acquisition system for internet-of-vehicles. In: Proceedings of the 16th IEEE/ACIS International Conference on Computer and Information Science (ICIS), Wuhan, China; c2017. p. 895–898.
9. Mangino A, Pour MS, Bou-Harb E. Internet-scale insecurity of consumer internet of things. ACM Trans Manag Inf Syst. 2020;11:1-24.
10. Lee T, Kim S, Kim K. A research on the vulnerabilities of PLC using search engine. In: Proceedings of the 10th International Conference on ICT Convergence: ICT Convergence Leading the Autonomous Future, Jeju,

Korea; c2019. p. 184–188.
11. Sarı T, Güleş HK, Yiğitol B. Awareness and readiness of Industry 4.0: The case of Turkish manufacturing industry. Adv Prod Eng Manag. 2020;15:57-68.
12. Gupta S, Sabitha AS, Punhani R. Cybersecurity threat intelligence using data mining techniques and artificial intelligence. Int J Recent Technol Eng. 2019;8:6133-6140.
13. Uzunov AV, Nepal S, Baruwal Chhetri M. Proactive antifragility: A new paradigm for next-generation cyber defense at the edge. In: Proceedings of the 2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC), Los Angeles, CA, USA; c2019. p. 246-255.
14. Smith KJ, Dhillon G, Carter L. User values and the development of a cybersecurity public policy for the IoT. Int J Inf Manag. 2021;56:102-123.