Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol: 56 Issue: 03:2023
DOI 10.17605/OSF.IO/T8YCW

INTERNET OF THINGS (IOT) SECURITY AND PRIVACY

SARFRAZ NAWAZ

Ph.D. (Scholar) Computer Science, Superior University, Lahore, Pakistan, and working as Lecturer CS at Govt. Graduate College, Kamoke, Gujranwala. E-mail: ranasarfraznawaz@gmail.com

MUHAMMAD IMRAN TARIQ

Department of Computer Science, Superior University, Lahore, Pakistan.

SYED PERVEZ HUSSNAIN SHAH

Ph.D. (Scholar) Computer Science, Superior University Lahore, Pakistan, and working as Lecturer IT at Lahore Leads University, Pakistan. Correspondence Author E-mail: Pervez.it@leads.edu.pk

TASKEEN

M. Phil (Scholar), The University of Sialkot, Pakistan, and working as SST (IT) at GGHS Marakiwal.
E-mail: taskeen546@gmail.com

AMNA IQBAL

Ph.D. (Scholar) Computer Science, Superior University Lahore, Pakistan.
Email: amnaiqbal962@yahoo.com

ZAINAB-UL-RIDA

M.Phil. (CS), Lecturer at International Institute of Science, Arts and Technology Gujranwala.
E-mail: zainabrida79@gmail.com

Abstract

The Internet of Things (IoT) contains intelligent objects that are comprised with various types of sensors, networks, electronics devices and process technologies that are integrated and work altogether, where the effective and intelligent services are provided to the users. Smart Cities have been proposed as a solution to urban problems, where the people of that city can live with more comfortable by using the innovative technology. The purpose of this paper is to provide thorough analysis of IoT technology, with major focus on privacy and security risks, attacks surfaces, vulnerabilities. Although the researchers are conducting studies on the services offered and challenges of IoT to make the Smart Cities effective. There is still some space between theory and practical of using Information and Communication Technology, (ICT). In order to highlight the basic requirements and concerns of users in the area of security and privacy, the requirements and problems of IoT users have been defined. In order to conduct this IoT privacy and security study, a systematic literature review is conducted using electronic databases and other sources to search for all articles that met specific criteria, enter information about each research into a personal database, and then create summary tables. Body of research. Consequently, the paper summarizes recent advances in IoT privacy and security, highlights outstanding issues, and suggests topics for further research.

Keywords: IoT, ICT, Internet of Things, Information Security, Privacy**,** Smart Cities, Threats, IoT Attacks, Data Security

Nomenclature

IoT	Internet of Things
ICT	Information and Communication Technology
SLR	Systematic Literature Review
OWASP	Open Web Application Security Project
SC	Smart City
SAST	Static Application Security Testing
CPS	Cyber Physical System
IoMT	Internet of Medical Things
VPN	Virtual Private Security
IP	Internet Protocol
RFID NFC	Radio Frequency Identification Near Field Communication
MII	Mobile Interface Insecurity
LPS	Low Physical Security
UIoTS ACM ECC DDoS DS OT QRC	Urban Internet of Things System Association for Computing Machinery Elliptic Curve Cryptography Distributed Denial of Service Data Security Optical Tag Quick Response Code

1. INTRODUCTION

In this modern era, the security and privacy of IoT is a serious issue. The rapidly growing field of IoT, as the IoT devices become more prevalent in our homes, businesses, and cities, the need for robust security and privacy measures becomes increasingly important. This review paper will explore the current state of IoT security and privacy, highlighting key challenges and potential solutions. One major challenge in IoT security is the lack of standardization among devices. Many IoT devices are developed by small or emerging companies with limited resources, which can make it difficult for them to implement strong security measures. Additionally, these devices often use proprietary protocols and communication methods, which can make it difficult for security researchers to identify and address vulnerabilities.

The sheer quantity of devices being linked to the internet is a major issue as well. By 2020, there are likely to be billions of IoT devices in use, making it more challenging to guarantee that each one is safe. The fact that many IoT devices are built more for convenience and usability than security complicates things even more. Several potential solutions have been proposed to address these issues. One approach is to develop industry standards for IoT security and privacy, such as the IoT Security Foundation's "Code of Practice for IoT Security." This would ensure that all IoT devices meet a certain minimum level of security. Additionally, there have been calls for increased government regulation of IoT security, such as the proposed IoT Cyber security Improvement Act in the United States. Another approach is to focus on securing the communication channels between IoT devices. This could include using encryption and secure protocols to protect data in transit, as well as implementing secure provisioning and device management methods to ensure that only authorized devices can connect to a network. Finally, there is growing interest in using machine learning and artificial intelligence to improve IoT security. This could include using machine learning algorithms to detect and respond to unusual network activity, or using AI to identify and mitigate vulnerabilities in IoT devices.

Overall, IoT security and privacy is a complex and rapidly evolving field. While there are many challenges to be addressed, there are also a number of promising solutions that can also help to increase the privacy and security of IoT devices. As IoT continues to grow and advance, it will be important for researchers, industry leaders, and government regulators to work together to ensure that these devices are secure and that user privacy is protected. The IoT is gaining ground in all facets of the contemporary world. The Internet of Things (IoT) is emerging as a global, all-encompassing network where everything will be connected to the Internet thanks to the never-ending advancements in technological innovation. IoT is a hot investigation area with boundless opportunities that is constantly growing. The vastness of minds has brought us quite close to transforming the existing type of web into a modified and coordinated variation. A ground-breaking data source will be made easily available if all of the devices that internet service providers benefit from are connected, whether by wire or remotely. An innovative concept is the idea of enabling connections between intelligent devices.[1].

A smart city is a mind throwing biological system described by the escalated utilization of data and Information & communication technology (ICT), expecting to make urban communities more appealing and more supportable. This field of ICT or IoT has the big opportunity for the business point of view because it is the emerging technology of the current age. The significant partners incorporate application designers, specialist organizations, residents, government and public specialist organizations, the examination local area, and stage engineers. Besides, the cycle of smart city comprises of various ICT advancements, facilities, and supportability, applications for developing residents. Therefore, IoT frameworks will play a basic part in the organization of enormous scope heterogeneous frameworks[2]. The "Smart City" idea has gotten amazingly famous in research writing and global strategies. This idea basically tackles a plenty of IT advancements hitting us at amazing speed to make urban communities more astute for the residents of that area. Urban communities and metropolitan territories contain about portion of the aggregate total populace. The metropolitan populace expansion for the last not many years has been unfavorably influencing amount and nature of administrations gave to the residents. The growth rate are increasing fast, consequently the services offered by the administrative authorities are not adequate to accomplish their current requirements. Some services are still time consuming and resources wasting. As current age is the age of technology, so the Smart Cities are the best solutions for the citizens of those areas where these types of problems exist. Smart cities are the mega projects; therefore any government of the city takes the initiative to build Smart Cities. In some areas of the different countries both the government and the private partnership work together to build smart cities to facilitate their citizens. ICT is main technology that is deployed in smart cities [3].

1.1 Privacy

Security is "an umbrella phrase, hinting to a large and distinct assemblage of linked things," according to Solove. According to Privacy International, security is a multidimensional concept that can be divided into four parts: 1) body, 2) correspondences, 3), domain, and 4) data. Real security is centered on people having protection from any outside harm. The supporting of the data that is brought between two gatherings over any channel is at the heart of exchange security. This includes phone, mail, and email. Setting boundaries or cutoff points on real estate, such as the house, workplace, and public places, is related to regional security. Data security refers to the protection of private information gathered and managed by a body, such as medical records, and related cards. [4]

1.2 Privacy Threats

These days, it is significantly harder for us to hold our security, as the Internet of Things advancements assume control over our day by day lives. Crashes over how connotations can acquire to particular information are inevitable, and IoT will add to this. Ziegeldorf's writing audit [84] lists the most well-known security dangers in IoT:

- Identification is the main risk that connects an individual element and an identifier, such as a name and address
- Localization and following are risks associated with discovering someone's whereabouts using different tools, such as a GPS, online traffic, or mobile phone area.
- In internet business, profiling is mostly used for customization (for example in bulletins and commercials). Instead, organizations set up information about people to determine interests through connections to various profiles and data sources.
- Interaction and introduction refer to the variety of clever strategies and improved methods for establishing connections with frameworks and presenting input to customers. When personal data is exchanged between framework and clients, this poses a threat to security.
- Lifecycle improvements take place when an IoT device is purchased, used by its owner, and finally destroyed. Although there is a possibility that all data is assumed to be wiped by the item, clever devices frequently retain a significant amount of knowledge about their individual set of experiences during their whole lifespan. Individual images and recordings may be included in this, and there may not always be an unending supply of them.
- Inventory attacks include unauthorized access to and collection of data on the existence and characteristics of certain items. Criminals can casing the property using stock information to find a safe moment to break in;
- Linkage involves joining different frameworks; when these are joining to join different information sources, there is a risk of unauthorized access and privacy breaches.

1.3 Security

The Data security (DS) is the abbreviation for the approach and ways of thinking that are used to ensure data, information, and framework. When it comes to information security, ensuring means preventing unauthorized access, usage, disturbing impact, disclosure, adjustment, or annihilation. There are three main principles for data security that might be thought about. They include respectability, accessibility, and privacy. Accountability has evolved into a more commonplace standard and is occasionally listed among the three principles by security organisations for companies like Combitech AB, etc.[5]

There are some huge challenges in different fields like health sector, transport systems, education systems, and power management systems, waste management, crime control and management system etc. The IoT provides the best solutions of those problems facing in various disciplines in the smart cities effective environment. There are various obstacles to build smarts city environment the major is funding for smart city projects and the some administrative and government issues as approvals of competent authorities. To educate the people of smart cities is also the issues which need to be addressed in efficient manner. [6]

The key objectives of this study are to understand the basics concepts of IoT, its applications areas where it deploys for the betterment of people of the cities. IoTs in the smart city is the major area covered in this review paper. This article is managed firstly the IoTs concepts, smart city environment its structure, major components, applications secondly issues, challenges and further discussed some areas where more work are required. Web users' interfaces are built up to communicate with monitors or operate the Internet of Things (IoT) devices that have also undergone inspection. The list of significant 10 vulnerabilities has been detailed by "The Open Web Application Security Project" (OWASP) [7] as indicated. Web interface security issues, insufficient authorization or authentication, unreliable network services, lack of transport encryption, and more. Five privacy concerns, five cloud interface security flaws, seven mobile interface security (MII) flaws, eight inadequate security configuration flaws, nine software or firmware flaws, and ten low physical security flaws (LPS).[8]

2. LITERATURE REVIEW

Ruchi Parashar and other describe IoT, which is model where objects can be furnished with distinguishing, detecting, networking and handling capacities that will permit them to communicate with each other and with different devices in secure manners. There are lots of services which can be completed over the Internet. Through the internet technology all the world is at single click. In this article the authors explain the current research state that has been conducted on the IoT sytem. The researchers use some techniques as deeply examine the literatures, present trends of IoT. They also describe the some challenges in IoT that endanger IoT dispersion in some area. Researchers talked about IoT architecture. There are five layers: business layer, application layer, processing layer, processing layer and identification layer. The business layer is the first layer. Determining which applications can be used in the Internet of Things is the main purpose of layers.

The Researchers describe the technology that enabled IoT. They explain three types of technology, one is NFC, RRFID and another is OT and QRC, and third is Bluetooth low energy which is the latest technology.The authors conclude that the internet has become the main factor that changed our life. And lot of research is required in the field of IoT. [9] The Researchers argue in the article that the novel cutting edge technology is the IoT that enables the connectivity of digital world. The scope of this research is IoT in the small city environment. The smart of IoT services and the big data analysis are empowering the smart city initiatives in the whole world.[2] In this paper the researcher emphasis explicitly on an Urban IoT system. They carried out cause because this is the general application area of IoT. The Urban IoT System (UIoTS) is to develop and explore the vision of Smart City. The main objective of this research is to bring the advancement in communication technology for value added services in city administration and the people living in that city.[10] The Authors argue that Smart Cities are very fast, safe, more green and flexible and the habitants of that Smart City are feeling level of comfort and enjoying the facilities provided in that area. Later on the Authors discuss the various components of Smart City. The key elements are Architecture, Buildings, Transportation system, Healthcare, Energy, Technology, Government, Education, and Citizens. These elements work together to create the city a Smart City. ICT is effectively used to do this.[11]

This study highlights the need for thorough investigation of privacy risks and pitfalls in IoT. We divide this complex topic into four steps: First, we provide a formal foundation for talking about privacy in the IoT by clearly stating our definition of privacy and the reference model used. A brief examination of relevant privacy laws reveals glaring shortcomings and reinforces the demand for a thorough analysis of privacy issues. The second phase recognizes that the Internet of Things is constantly changing and cannot be summed up by the technology it is based on. Here, our descriptions of emerging features and technologies provide both a comprehensive and privacy-focused perspective on IoT's past, present, and future developments. Finally, researchers sum up findings. [14]

The IoT has a big part in the contemporary technology's fast growth. Data sharing is now simpler thanks to technology. Therefore, it is important to consider user data security. The research done for this article is therefore primarily concerned with the security of IoT technologies. So, as we've previously discussed, the Internet of Things is vulnerable to a number of assaults, including DDoS, password guessing, replay, and insider attacks. We've covered the authentication methods used for IoT because it's one of the initial security requirements that the technology must meet. The most popular methods for imposing authentication are one-time passwords, mutual authentication based on ECC, ID verification, certificate verification, and block-chain. Recent authentication systems have been compared, and we have determined that the majority is based on block-chain. [15] Data security and privacy in the connected society are being challenged by the exponential increase in data availability and sensitivity in recent years. The Internet and cloud spaces' adoption of an extensive range of technologies, services, and standards raises the possibility that security concerns may only get worse over time. Figure 1 illustrates the sharp growth in security risks over time, as a result of the development of new instruments for launching attacks in safe cyberspace. The information required to start an attack, however, is decreasing rapidly as security assaults get more sophisticated. To provide complete and reliable data protection, privacy protection and security measures must be equally suitable. [16]

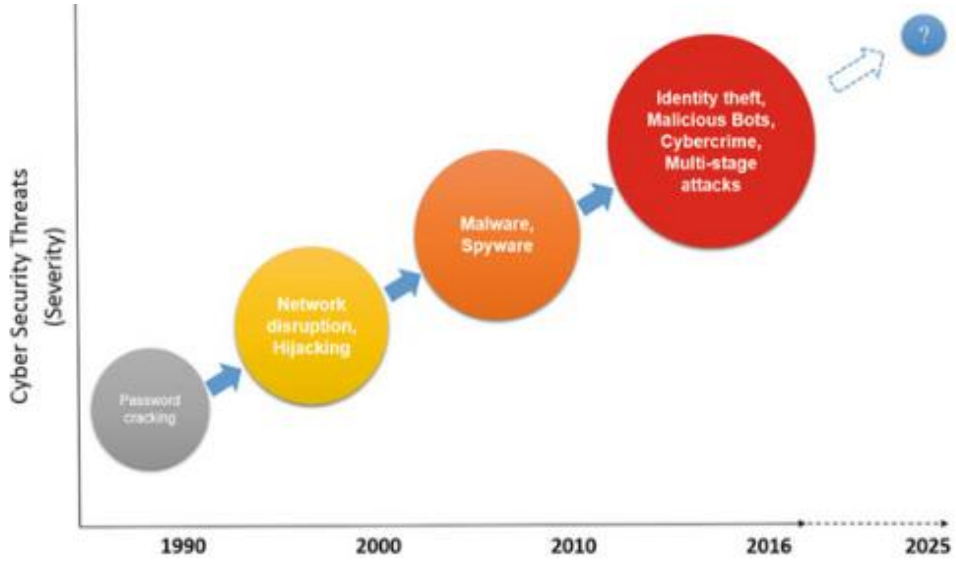


Fig.1: Shows the Growth of various Threats

3. METHODOLOGY

In this paper, the SLR procedure is adopted and PRISMA [12] method for the applications of IoTs offer in the Smart Cities. This research is comprised with the three main steps one is the planning step and second is conducting-step and the final is reporting-step. These are all mentioned in subsequent figure 2, and each step explained separately in detail

3.1 Step-1 Planning

All through this step, we decided the principle point of the review and did the accompanying exercises that clarified each progression in detail. The main objectives of this STR conducting are to identify the security and privacy offered in Smart Cities by using IoTs technologies. Therefore we prepared some research questions to analyze this Smarts City's environment.

The main research questions are as under

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?

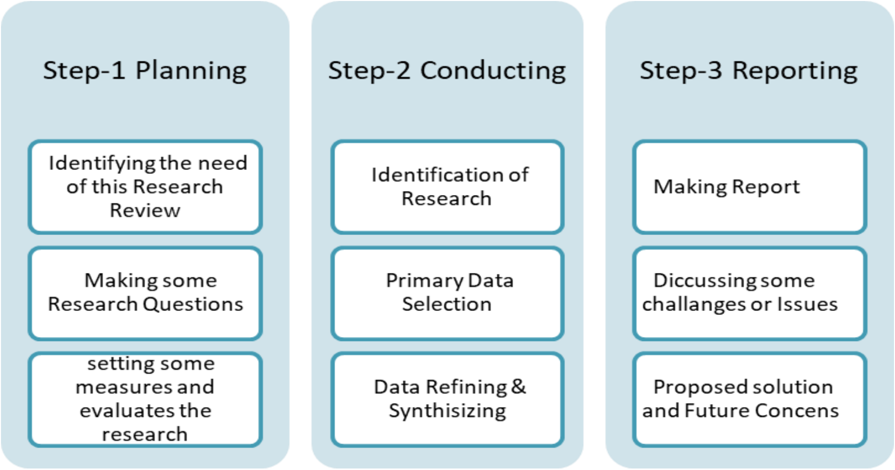

Step-1 Planning
Identifying the need of this Research Review
Making some Research Questions
setting some measures and evaluates the research
Step-2 Conducting
Identification of Research
Primary Data Selection
Data Refining & Synthisizing
Step-3 Reporting
Making Report
Diccussing some challanges or Issues
Proposed solution and Future Concens

Fig. 2: Systematic Literature Review Steps & Activities

3.2 Step-2 Conducting Review

This research began via looking through the surviving writing by utilizing general Keywords to get whatever number applicable papers as could reasonably be expected. A few online data sets were utilized to cover a wide scope of scholastic distribution. The online data sets were utilized are: Google Scholar, Springer, IEEE Explorer Access, Research gates, ACM Digital Library, and also other Web of science. These data sets are viewed as applicable and give high effect factor distribution. To play out the programmed search, focus on “Security and Privacy of *the Internet of things IoT*” and some related issues were distinguished dependent on the examination question of this review. Fig 3 displays that how the data of research papers collected from the electronic database.

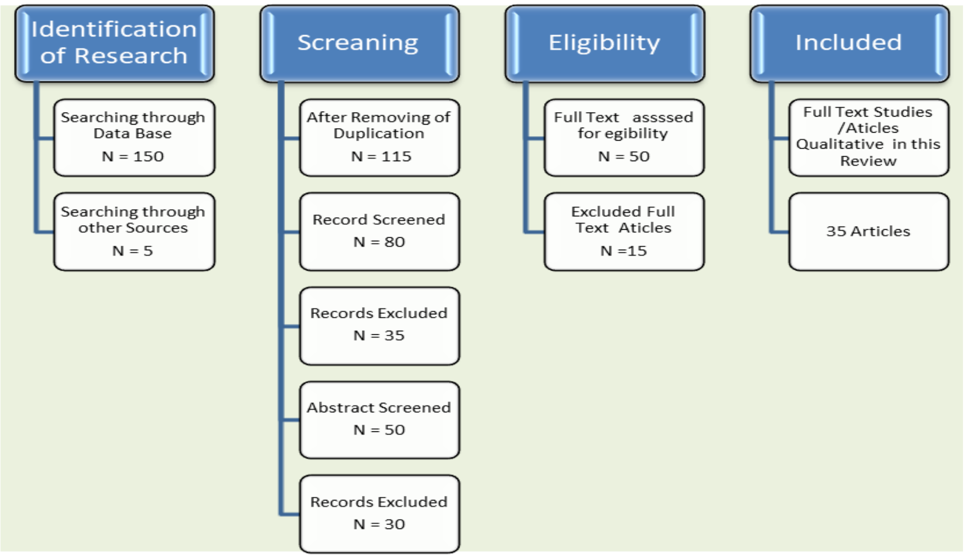

Identification of Research
Searching through Data Base N = 150
Searching through other Sources N = 5
Screaning
After Removing of Duplication N = 115
Record Screened N = 80
Records Excluded N = 35
Abstract Screened N = 50
Records Excluded N = 30
Eligibility
Full Text asssssed for egibility N = 50
Excluded Full Text Aticles N =15
Included
Full Text Studies /Aticles Qualitative in this Review
35 Articles

Fig. 3: Flow of PRISMA Technique

The table 1 here describes the details of all final consideration of research papers, book chapters, and other related material with citation reference published year and the name of all publishers and data sources. There are 35 selected articles of the most relevant to our study of the famous electronic data base.

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]

The Fig.4 shows the information of table 1 in term of graph. The publisher names are at the horizontal plane and published year are at vertical plane. The range of selected material under study is 2008-2024.

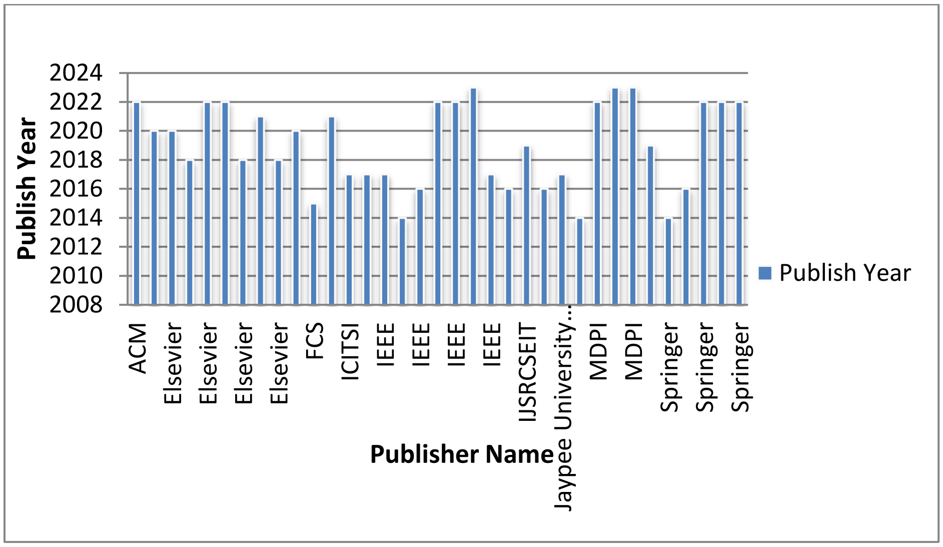


Fig. 4: Graph for Publisher and year

Authors summarize the total number of publication considered according to publishers in table 2. There 14 different publishers are included in this review. The maximum numbers are consideration IEEE and Elsevier as 9 and 8 respectively.

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

The Fig.5, graph shows the information of table 2. The publisher names are at the horizontal plane and the numbers of publications of relevant are at vertical plane. IEEE shows the highest in the graph due to larger value.

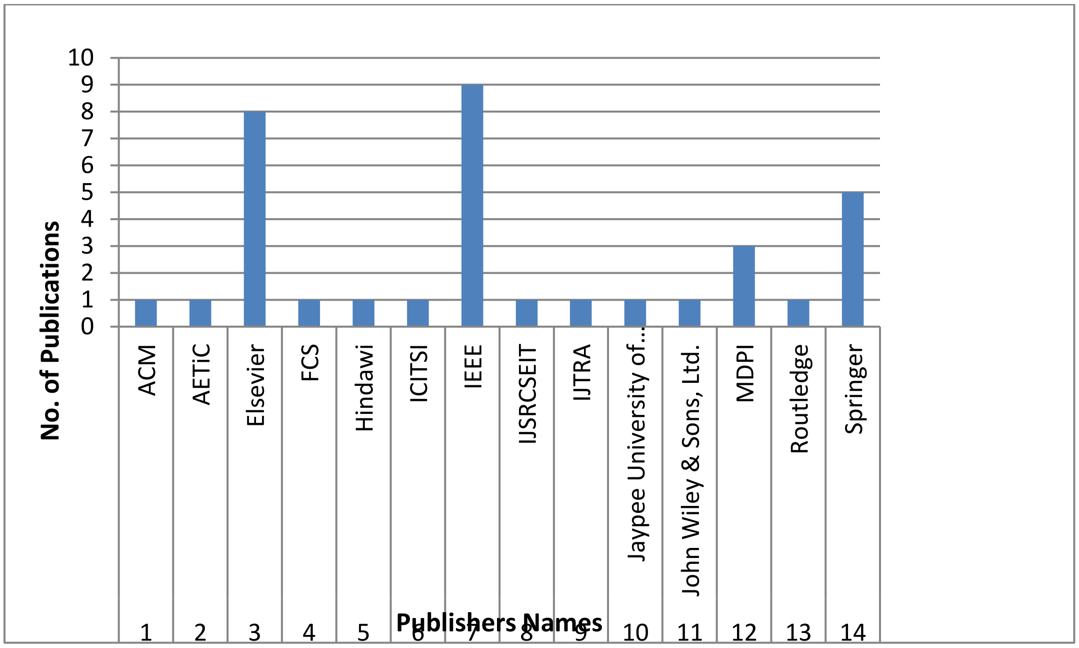


Fig. 5: Graph of No. Publication and Publishers

3.3 Step-3 Reporting

Studies identified in the reviews were analyzed against the background of identified research questions using thematic analysis, which systematically identifies domains of security, privacy applications and services. Some the challenges, threats and other related issues are also determined to build smart city environment in more secure and trustable order to answer the research questions. Then the report is built to answers the research questions.

4. RESULT AND DISCUSSION

This section shows some findings to according to Systematic Literature Review of the Security and privacy in the Smart Cities environment, some security application and services offered in the scenario of modern digital era. The table 3 shows the major security issues those have been found in the selected research papers as in IoTs Smart City environment [13].

Table 3: Major Security Issues in IoTs

Sr. No.	Referenced	Data Privacy	Authentication	Availability of Data	Data Integrity	Data Access	Data Confidentiality	Identification	Access Control	Devices Security	Others issues
1	[1]	c	c	c	n	c	c	c	c	c	c
2	[2]	c	n	n	c	c	c	n	n	c	c
3	[4]	c	c	c	n	c	c	n	c	c	c
4	[5]	n	c	c	c	n	n	c	c	c	n
5	[6]	c	c	n	c	c	c	n	c	n	c
6	[7]	c	c	c	c	n	c	c	n	n	c
7	[8]	c	c	n	n	c	c	n	n	c	c
8	[10]	c	n	c	c	c	c	n	c	c	n
9	[12]	c	c	n	c	c	n	c	c	c	c
10	[13]	c	c	c	c	c	c	c	c	c	n
11	[14]	c	n	n	n	c	c	c	n	c	c
12	[15]	c	c	c	c	n	c	c	c	c	c
13	[16]	c	c	n	c	n	c	c	c	c	n
14	[17]	c	c	n	c	c	c	c	c	c	c
15	[21]	c	c	n	c	c	c	n	c	c	c
16	[22]	c	c	c	c	c	c	c	c	c	c
17	[23]	c	c	n	c	n	c	c	n	c	c
18	[24]	c	c	c	c	c	c	c	c	c	c
19	[25]	c	c	n	c	c	c	c	c	c	c
20	[30]	n	n	c	n	c	n	c	n	n	c
21	[31]	C	c	c	n	c	n	c	c	n	c
22	[32]	c	n	c	c	c	n	c	n	n	c
23	[33]	c	c	c	c	c	c	n	c	c	c
24	[34]	c	c	c	c	c	c	c	c	c	c
25	[35]	c	c	c	c	c	c	n	c	c	c

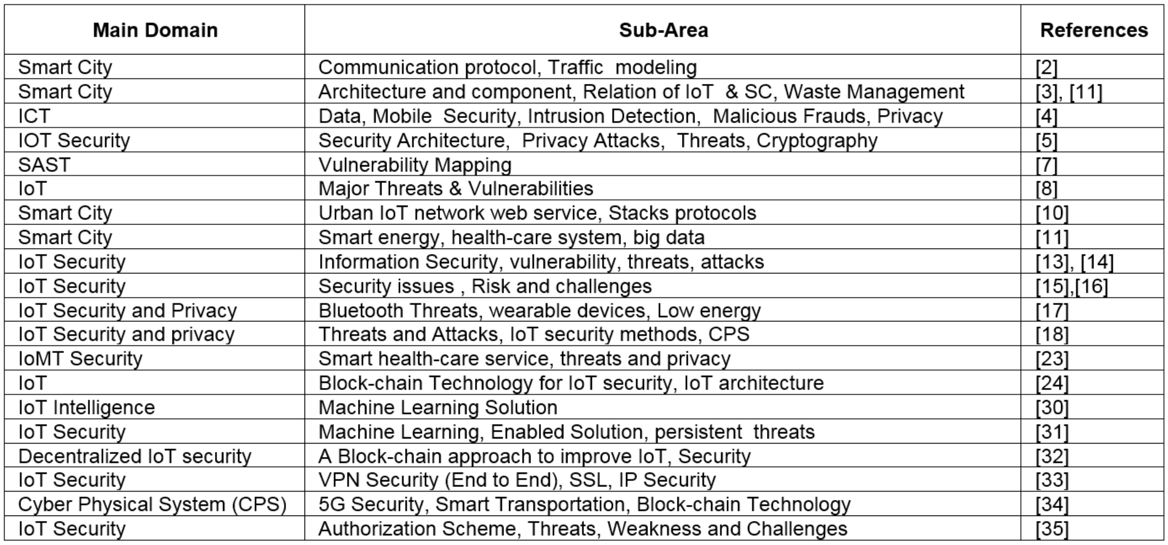
*c means reference papers have covered security issues while n means not covered.

Some security and privacy challenges are determined in the following table 4 and major domain of IoT Security and sub areas of security and privacy is given in table 5.

Table 4: Security & Privacy Challenges

Description	Security & Privacy Challenges	References
Big Data	Handling of big data in secured way on the IoTs Networks.	[10],[13]
Interoperability	Appropriate security solutions should not interfere with the operation of many connected devices in IoTs Network system.	[12]
Limitations of resources	Architecture of IoT, many nodes do not have enough storage capability, power, and processor and low speed connection. Hard to deployed security mechanism	[3],[9]
Maintain of Privacy	Some RFID having no any suitable authentication technique therefore, it can be control and identified by the attackers.	[4]
Scalability	The IoT network comprises of numerous nodes. The security tools proposed in IoT.	[1],[7]
Trust building	Due to absence of central controlled administration for IoTs infrastructure, trust management is the challenge.	[3][5]
Autonomic control	Other than the conventional communication system, IoTs based system required automated configuration, operation and management.	[2],[6]
Access control	The Access control is necessary s for IoT devices located on in any place near or remote.	[8], [9]
Interruption or interference control	Monitoring of any abnormality in traffics on networks, the detection and avoidance is big challenge to avoid from different types of attacks.	[2], [12],[13]
Advance Persistence Attacks	Network- Physical, Application Layer Security	[31]
Design Issue	Network Layer Security	[32]

Table 5: Domain of IoT Security & Privacy



Main Domain	Sub-Area	References
Smart City	Communication protocol, Traffic modeling	[2]
Smart City	Architecture and component, Relation of IoT & SC, Waste Management	[3], [11]
ICT	Data, Mobile Security, Intrusion Detection, Malicious Frauds, Privacy	[4]
IOT Security	Security Architecture, Privacy Attacks, Threats, Cryptography	[5]
SAST	Vulnerability Mapping	[7]
IoT	Major Threats & Vulnerabilities	[8]
Smart City	Urban IoT network web service, Stacks protocols	[10]
Smart City	Smart energy, health-care system, big data	[11]
IoT Security	Information Security, vulnerability, threats, attacks	[13], [14]
IoT Security	Security issues , Risk and challenges	[15],[16]
IoT Security and Privacy	Bluetooth Threats, wearable devices, Low energy	[17]
IoT Security and privacy	Threats and Attacks, IoT security methods, CPS	[18]
IoMT Security	Smart health-care service, threats and privacy	[23]
IoT	Block-chain Technology for IoT security, IoT architecture	[24]
IoT Intelligence	Machine Learning Solution	[30]
IoT Security	Machine Learning, Enabled Solution, persistent threats	[31]
Decentralized IoT security	A Block-chain approach to improve IoT, Security	[32]
IoT Security	VPN Security (End to End), SSL, IP Security	[33]
Cyber Physical System (CPS)	5G Security, Smart Transportation, Block-chain Technology	[34]
IoT Security	Authorization Scheme, Threats, Weakness and Challenges	[35]

5. CONCLUSION

In this research the authors get some list of security and privacy issues especially in IoT based Smart Cities infrastructure. It is done through conducting Systematic Literature Review. IoT in Smart cities have now become the need of current age. The needs to get services at their door steps or in a manner where required minimum effort, less use of resources, saving their times, cost effective, reliable. All of above more secured in every aspect is the main objective. So this can be achieved through the use of ICT. IoT enabled Smart City having the capability to facilitate to people of that city. And by deploying security mechanism in efficient manner this can be achieved properly. As in this review the author finds the various areas, where more work are needed to make IoT services trustworthy for the betterment of living people. This research presents an overview of the most important IoT concepts, with an emphasis on the security concerns and difficulties associated with IoT devices. Threats and weaknesses that might prevent users from adopting IoT technology have been detected. In order to develop a reliable and secure platform which can increase consumer acceptance of the technology, we have highlighted a number of security and privacy challenges that the research community has to address. In order for people to use IoT devices to exchange and exchange information globally with assurance of trust and security, there is an urgent need for research centers in this field to address these security pitfalls and barriers in IoT based infrastructure.

6. FUTURE WORK

The most issue that is asking to be tended to is revamping the use of security in IoT for engineers without thorough learning of IT security. Planning and carrying out security in shows that is fundamental for planners to use is an outright necessity for the fate of IoT. Speed and cryptographic quality is especially fundamental in the Internet of Things.

However, the issue of security is equally pressing. Future research should assess the security insights identified with the IoT, and to see whether individuals will act to ensure their own security when using the IoT. In addition, we must determine whether they will respect and use administrative tools that explicitly prevent security intrusions by IoTs devices. Making IoT systems more secure, efficient and effective is a big challenge, especially handling big data in real time. Therefore researchers should focus on enhancing the security, integrity, efficiency and reliability of IoT based smart cities.

Acknowledgement

We appreciate to Dr. Imran Tariq for such a great and useful supervision throughout this work.

Conflicts of Interest

The authors declare that they have no conflicting interests to report in this work.

REFERENCES

1. Farooq, M., Waseem, M., Mazhar, S., Khairi, A., Kamal, T.: A Review on Internet of Things (IoT). Int. J. Comput. Appl. 113, 1–7 (2015). https://doi.org/10.5120/19787-1571
2. Mehmood, Y., Ahmad, F., Yaqoob, I., Adnane, A., Imran, M., Guizani, S.: Internet-of-Things-Based Smart Cities: Recent Advances and Challenges. IEEE Commun. Mag. 55, 16–24 (2017). https://doi.org/10.1109/MCOM.2017.1600514
3. Full article H. Samih (2019) Smart cities and internet of things, Journal of Information Technology Case and Application Research, 21:1, 3-12, DOI: 10.1080/15228053.2019.1587572
4. Hoepman, J.-H.: Privacy Design Strategies. In: Cuppens-Boulahia, N., Cuppens, F., Jajodia, S., Abou El Kalam, A., and Sans, T. (eds.) ICT Systems Security and Privacy Protection. pp. 446–459. Springer, Berlin, Heidelberg (2014)
5. Sharma, M., Sehgal, V.: Security and Privacy Mechanism in IOT. (2017)
6. Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., Zhao, W.: A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. IEEE Internet Things J. 4, 1125–1142 (2017). https://doi.org/10.1109/JIOT.2017.2683200
7. Li, J. (2020). Vulnerabilities Mapping based on OWASP-SANS: a Survey for Static Application Security Testing (SAST). *ArXiv, abs/2004.03216*.
8. Stout, W.M.S., Urias, V.E.: Challenges to securing the Internet of Things. In: 2016 IEEE International Carnahan Conference on Security Technology (ICCST). pp. 1–8. IEEE, Orlando, FL, USA (2016)
9. Parashar, R., Khan, A.: A SURVEY: THE INTERNET OF THINGS. 4, 7 (2016)
10. Zanella, A., Bui, N., Castellani, A., Vangelista, L., Zorzi, M.: Internet of Things for Smart Cities. IEEE Internet Things J. 1, 22–32 (2014). https://doi.org/10.1109/JIOT.2014.2306328
11. Mohanty, S.P., Choppali, U., Kougianos, E.: Everything you wanted to know about smart cities: The Internet of things is the backbone. IEEE Consum. Electron. Mag. 5, 60–70 (2016). https://doi.org/10.1109/MCE.2016.2556879
12. Oktaria, D., Suhardi, Kurniawan, and N.B.: Smart city services: A systematic literature review. In: 2017 International Conference on Information Technology Systems and Innovation (ICITSI). pp. 206–213 (2017)
13. Ogonji, M.M., Okeyo, G., Wafula, J.M.: A survey on privacy and security of Internet of Things. Comput. Sci. Rev. 38, 100312 (2020). https://doi.org/10.1016/j.cosrev.2020.100312

14. Ziegeldorf, J. H., Morchon, O. G. and Wehrle, K. (2014), Privacy in the Internet of Things: threats and challenges, *Security Comm. Networks*, 7, pages 2728– 2742, doi: 10.1002/sec.795

15. Azrour, M., Mabrouki, J., Guezzaz, A., & Kanwal, A. (2021). Internet of things security: challenges and key issues. *Security and Communication Networks*, *2021*, 1-11.

16. Varadharajan, V., Bansal, S. (2016). Data Security and Privacy in the Internet of Things (IoT) Environment. In: Mahmood, Z. (eds) Connectivity Frameworks for Smart Devices. Computer Communications and Networks. Springer, Cham. https://doi.org/10.1007/978-3-319-33124-9_11

17. Ziegeldorf, Sadhu, P. K., Yanambaka, V. P., & Abdelgawad, A. (2022). Internet of Things: Security and Solutions Survey. *Sensors*, *22*(19), 7433.

18. Azrour, Hassan, W. H. (2019). Current research on Internet of Things (IoT) security: A survey. *Computer networks*, *148*, 283-294.

19. M., Sadhu, P. K., Yanambaka, V. P., & Abdelgawad, A. (2022). Internet of Things: Security and Solutions Survey. *Sensors*, *22*(19), 7433.

20. Shokry, M., Awad, A. I., Abd-Ellah, M. K., & Khalaf, A. A. (2022). Systematic survey of advanced metering infrastructure security: Vulnerabilities, attacks, countermeasures, and future vision. *Future Generation Computer Systems*.

21. Allifah, N. M., & Zualkernan, I. A. (2022). Ranking security of IoT-based smart home consumer devices. *Ieee Access*, *10*, 18352-18369.

22. Rao, P. M., & Deebak, B. D. (2022). Security and privacy issues in smart cities/industries: Technologies, applications, and challenges. *Journal of Ambient Intelligence and Humanized Computing*, 1-37.

23. Keshta, I. (2022). AI-driven IoT for smart health care: Security and privacy issues. *Informatics in Medicine Unlocked*, *30*, 100903.

24. Kumar, N. M., & Mallick, P. K. (2018). Blockchain technology for security issues and challenges in IoT. *Procedia Computer Science*, *132*, 1815-1823.

25. Ziegeldorf, Zubaydi, H. D., Varga, P., & Molnár, S. (2023). Leveraging Blockchain Technology for Ensuring Security and Privacy Aspects in Internet of Things: A Systematic Literature Review. *Sensors*, *23*(2), 788.

26. Ashok, K., & Gopikrishnan, S. (2023). Statistical Analysis of Remote Health Monitoring Based IoT Security Models & Deployments from a Pragmatic Perspective. *IEEE Access*, *11*, 2621-2651.

27. Perwej, Y., Parwej, F., Hassan, M. M. M., & Akhtar, N. (2019). The internet-of-things (IoT) security: A technological perspective and review. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN*, 2456-3307.

28. Aversano, L., Bernardi, M. L., Cimitile, M., & Pecori, R. (2021). A systematic review on Deep Learning approaches for IoT security. *Computer Science Review*, *40*, 100389.

29. Ziegeldorf, Deogirikar, J., & Vidhate, A. (2017, February). Security attacks in IoT: A survey. In *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)* (pp. 32-37). IEEE.

30. Sarker, I. H., Khan, A. I., Abushark, Y. B., & Alsolami, F. (2022). Internet of things (iot) security intelligence: a comprehensive overview, machine learning solutions and research directions. *Mobile Networks and Applications*, 1-17.

31. Chen, Z., Liu, J., Shen, Y., Simsek, M., Kantarci, B., Mouftah, H. T., & Djukic, P. (2022). Machine learning-enabled iot security: Open issues and challenges under advanced persistent threats. *ACM Computing Surveys*, *55*(5), 1-37.

32. Qian, Y., Jiang, Y., Chen, J., Zhang, Y., Song, J., Zhou, M., & Pustišek, M. (2018). Towards decentralized IoT security enhancement: A blockchain approach. *Computers & Electrical Engineering*, *72*, 266-273.

33. M., Monem, A. A., & Shaalan, K. (2020). Hybrid end-to-end VPN security approach for smart IoT objects. *Journal of Network and Computer Applications*, *158*, 102598.

34. Rajawat, A. S., Goyal, S. B., Bedi, P., Verma, C., Ionete, E. I., & Raboaca, M. S. (2023). 5G-Enabled Cyber-Physical Systems for Smart Transportation Using Blockchain Technology. *Mathematics*, *11*(3), 679.

35. Khan, A., Ahmad, A., Ahmed, M., Sessa, J., & Anisetti, M. (2022). Authorization schemes for internet of things: requirements, weaknesses, future challenges and trends. *Complex & Intelligent Systems*, *8*(5), 3919-3941.