NIPES

Journal of Energy Technology and Environment

Journal homepage: www.nipesjournals.org.ng

IoT Device Security, Privacy, and Risks in Smart City Environments

Omosigho O. Moses* and Ehizuenlen E. Prudence
Department of Computer Engineering, University of Benin, Benin City, Edo State, Nigeria
*Corresponding Author: moses.omosigho@uniben.edu

Article information

Article History
Received 17 April 2024
Revised 1 May 2024
Accepted 22 May 2024
Available online 31 May 2024

Keywords:
IoT Device, Smart City, Security, Privacy, Risks

https://doi.org/10.5281/zenodo.11412563

https://nipes.org

Abstract

The rapid adoption of the Internet of Things (IoT) in smart cities has opened up unprecedented opportunities for efficiency and creativity in urban cities. But the incorporation of these gadgets into urban infrastructure raises significant concerns regarding security, privacy, and associated risks. This paper examines the vulnerabilities inherent in IoT devices, including insufficient authentication mechanisms, susceptibility to malware attacks, and the potential for unauthorized access. It investigates how these flaws could be exploited to compromise the security and veracity of data gathered by IoT devices, endangering public safety as well as vital infrastructure. This study also examines how IoT adoption affects privacy in smart cities and offers solutions for preserving people's right to privacy within an IoT smart city ecosystem. This paper advocates for a multi-disciplinary approach that includes policymakers, technology developers and researchers, to reduce risks, safeguard individual rights and build trust in the ever-changing landscape of city IoT deployments

1. Introduction

Over the past several years, there has been a noticeable growth in the quantity of Internet of Things (IoT) devices. An IoT device uses direct internet connections to provide data and communication technology (ICT) services [1]. Human relationship with its surroundings has been deeply impacted by this action. It has resulted in the ability to work more quickly on numerous daily activities and to become more connected and efficient in their professional procedures. IoT devices help regulate and optimise urban infrastructure, which is why they are essential to smart cities. However, because IoT is widely used in smart cities, there are serious concerns about potential risks, security, and privacy associated with IoT devices. [4]. According to research, IoT devices are vulnerable to cyber-attacks because of the high level of interaction and data flow between individuals, devices, and sensors [5],[6],[7],[8],[9]. Cybercrime [10], data breaches [11], and destructive activities [12] are risks that are increased when sensitive data and information are shared without adequate security measures.

IoT devices gather and retain enormous quantities of data, which raises significant privacy concerns. [13]. International Data Corporation (IDC) estimates projected that 41.6 billion IoT-enable devices will be in operation by 2025, producing 79.4 Zettabytes of data. [14]. Researchers need to examine the security and privacy protocols that IoT devices now employ for collecting, sending, storing, and exchanging data. [13], [4]. The threat of data breach and misuse is increased by the absence of strong

legal and data security frameworks, putting individuals at risk of identity theft, profiling, and other privacy breaches. [16]. The IoT lacks well-defined prevalent standards that dictate how diverse components of technology should interact [17]. The absence of global standards would make it difficult for makers of IoT devices to provide comprehensive security solutions [18].

IoT-based smart devices uses cloud computing technologies to get over drawbacks such low power, low capacity, and limited processing power, which may be used to obtain unauthorized access to data. Policy makers, urban planners, technology developers, and community stakeholders need to prioritize security, privacy, and risk management when creating, implementing, and overseeing IoT devices in smart cities because of these worries. In order to provide a safer, and more sustainable usage of IoT devices across all use cases, this paper analyses and summarizes solutions to improve IoT device security and privacy by integrating robust security, risk management, and threat mitigation capabilities into standardized IoT technology implementation. Numerous generic functional IoT designs are built around a simplified Open System Interconnect (OSI) model as described in the literature such as in [34[, [35], [36], and [37]. Figure 1 illustrates the three-layer and five-layer IoT architectures of a typical IoT architecture. The three-layer architecture has perception/sensing, network, and application, while the standard method is extended to five layers of architecture which has application, middleware/processing, transportation/network, perception/sensing, and business. Every layer is susceptible to different types of attacks and presents a unique set of security and privacy concerns. IoT reference designs commonly employ a number of popular communication protocols, such as Wi-Fi, LTE, Ethernet, BLE, and ZigBee. [43, 44, 45, and 46].

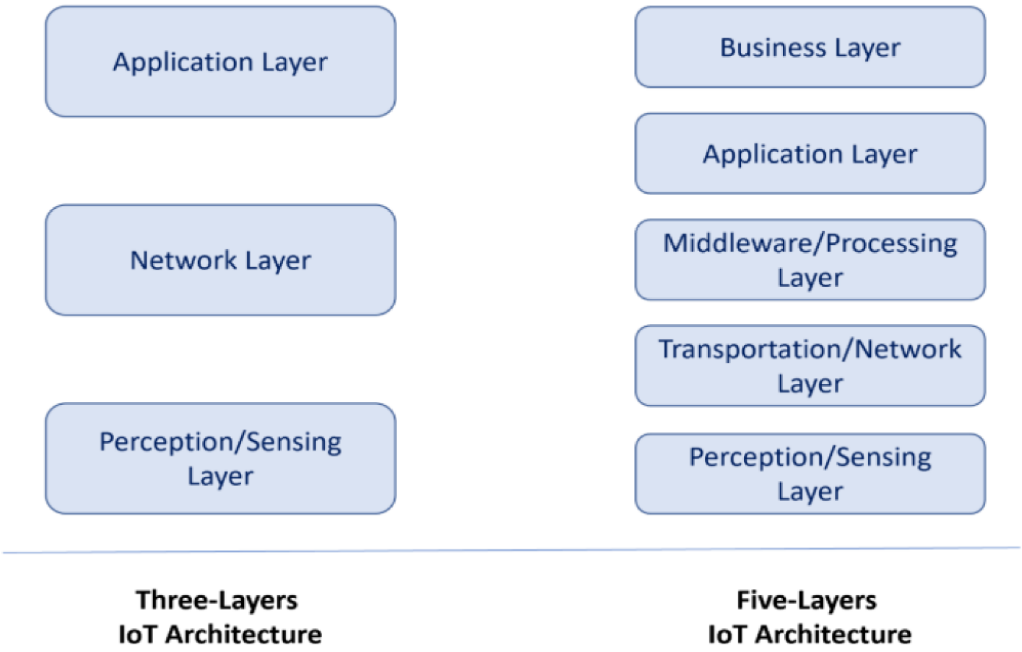

Figure 1. Layered IoT architecture

The creation of a common framework for efficient communication, data collection, analysis, and regulation of the smart city environment is one of the numerous IoT infrastructure types recommended for smart cities. [47], [48].

a. Perception/Sensing Layer: this layer of the IoT architecture employs the use of sensors, actuators and other devices to gather data directly from the physical world. It comprises every piece of tangible equipment, including sensors, GPS modules, IP cameras, Fitbits, RFID tags, and RFID

readers [49], [50]. This layer consists of physical security, real-time monitoring, and immediate data collecting. It plays an essential role in collecting data on the environment, devices, and events. This data helps the IoT system understand changes and make intelligent decisions. [51].

b. Network Layer: this layer enables data exchange and communication between IoT devices and other network segments. This network layer is a crucial part of the IoT architecture. [52]. Components of the network layer includes: ZigBee Wireless communication technologies Wi-Fi [53], Bluetooth [54], and 3G/4G/5G [53] etc. The IoT's reliability, scalability, and connection are provided via the network layer. [55]. Using a range of protocols, packet forwarding and routing are handled by the network layer. [56]. Specialized protocols including IEEE 802.11, MQTT, TCP/IP, CoAP, and wireless local area networks are frequently used by Internet of Things devices. [57].

c. Application Layer: this is top layer of the IoT's architecture and it manages and enables communication between end user applications and the devices and networks that make up the IoT stack. [58]. The layer incorporates mobile applications, web interfaces or software applications, cloud services and storage, processing and analysis of IoT device data, data aggregation and business logic governing how IoT devices work and respond to different conditions. [59]. Access control mechanisms and features for device management are included in this layer to help prevent unauthorized access to sensitive data and smart devices [60].

[23] The Privacy And Security Concerns Associated With Smart Cities Were Examined By The Researchers. The Study Addressed Five Concerns And Proposed Solutions To Help Anticipate Costly And Disruptive Changes In The Future. The Problems Included Managing Cascaded Failures With Smart Networks, Using Artificial Intelligence (Ai) Efficiently, Developing Robust Data-Sharing Protocols, Safeguarding A Network With Wide Attack Surfaces, And Maintaining The Privacy Of High-Dimensional Data. Prior To Building, The Experts Recommended Additional Investigation Into The Challenges Associated With Smart Cities.

[24], [25] The Study Identified Information Security Flaws In The Way Smart City Infrastructures Manage And Retain Personal Data, Reviewed A Range Of Security, Privacy, And Risk Issues In The Context Of Smart Cities, And Developed A Framework For Communication Between Them. It Also Provided A Helpful Summary Of Significant Literary Works. The Study's Results Provided Academics And Practitioners With A Framework And An Educated Research Strategy. [26] This Study Discusses The Primary Uses For Smart Cities, The Security Needs For The Iot Systems That Support Them, And The Importance Of Privacy And Security Considerations While Creating Smart City Apps. In Order To Enhance Future Performance, The Study Focused On Research Possibilities That Still Need To Be Taken Into Consideration, Along With Some Security And Privacy Solutions That May Be Employed To Construct Safe Smart City Systems. This Follows The Discovery Of Many Privacy Concerns And Security Flaws Pertaining To Smart Cities. Concerns Regarding Iot Security And Privacy Have Been Brought Up In Research Articles Such As In [27] And [28]. Along With A Few Iot Security And Privacy Obstacles, The Authurs Studied A Range Of Fundamental Security And Privacy Issues, Including User Privacy, Data Protection, Verification, Authorization, And Restricted Access [29].

[30] [31] The First Section Of Their Report Is Based On A Survey That Gives Readers A Thorough History And Overview Of Smart Cities. The Second Section Discusses The Need To Build Strong And Secure Smart Cities As Well As Privacy And Security Issues With Currently Available Smart Applications. The Third Section Provided An Overview Of The Defensive Technologies Currently

In Use. While The Final Section Discusses The Open Research Topic And Potential Directions For Further Investigation. [32, 33]. The Study Examined A Variety Of Basic User Privacy, Data Protection And Verification, Permission, And Restricted Access Which Are Just A Few Of The Iot Security And Privacy Obstacles And Concerns.

[34]The Study Was Organised Around A Number Of Key Themes Within Smart Cities Research: Privacy And Security Of Mobile Devices And Services Operational Vulnerabilities For Smart Cities; To Improve Security And Privacy, Operational Threats For Smart Cities. The Study Posited That Smart City Residents Can Face Security And Privacy Issues Due To Smart City Devices And App Vulnerabilities While For Cloud Platform Security - Threats Could Include Data Leakage, Malicious Insider Threats, Insecure Api, Dos, Malware Injection Attacks, System And Application Vulnerabilities. It Stated However, That Without Perceived Adequate Vulnerability Identification Measures And Mitigating Security Protection And Privacy, The Public Might Hesitate To Use Smart City Devices And Mobile Applications.

2. Methodology

To begin, two research questions were first formulated using the Common Vulnerabilities and Exposures (CVE) website (http://www.cvedetails.com) to classify, assess IoT device vulnerabilities [61], and narratively investigate existing literature on IoT device security, privacy, and application hazards in smart cities. The current study aims to address the following research questions (RQs):

a. RQ1: How vulnerable are IoT devices in smart cities to cyber-attacks, and what are the most common attack vectors?

b. RQ2: What are the privacy and risk challenges of the data obtained IoT devices in smart cities, and how may these issues be resolved?

Next, the aim of the research question (RQ1) was to define the vulnerability assessment which is the process of analyzing the IoT device system for security threats called vulnerabilities and assessing the potential impact of those vulnerabilities. [59]. The classified vulnerabilities are divided into 13 types: denial of service (DOS SQL injection, code execution, and cross-site scripting (XSS) are examples. Out of all the data collected between 2014 and 2023, only the data from 2023 were utilized to provide the basic data for the study. Vulnerabilities that arise independently in mobile apps and operating systems (e.g., Windows, Linux) are excluded from the basic data.

With the necessary information in mind, the following questions were considered:

i. Is the vulnerability due to IoT devices or IoT-related?
ii. Is it the operating system of IoT devices, or vulnerability in the software that runs on them?
iii. Is the vulnerability software-related?

For the purpose of confirming the study, vulnerabilities that occur in mobile applications (Android, iOS, etc.) were omitted, while only mobile device vulnerability data was included. The reason for this is that it’s a waste of resources to invest in mitigating vulnerabilities that won't have any significant impact on the behavior of the system because not all vulnerabilities carry the same risk. Figure 2 to Figure 4 represents the vulnerabilities obtained from Common Vulnerabilities and Exposures (CVE) website (http://www.cvedetails.com) data by types, impact types and types respectively.

Year	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	File Inclusion	CSRF	XXE	SSRF	Open Redirect	Input Validation
2014	832	627	304	1099	207	3	266	67	10	48	535
2015	1073	1104	221	776	152	6	249	50	8	46	382
2016	1214	1174	97	497	99	12	88	41	16	33	532
2017	2494	1555	505	1500	283	155	334	109	57	97	972
2018	2100	1748	504	2043	573	112	479	189	118	85	1285
2019	1213	2057	554	2389	491	127	560	139	103	122	927
2020	1222	1903	466	2203	441	110	416	119	132	101	832
2021	1677	2566	744	2726	560	93	520	126	197	133	704
2022	1886	3420	1790	3407	735	101	769	127	235	147	823
2023	1724	2813	2159	5179	808	137	1398	138	248	188	786
2024	371	587	413	1001	155	33	244	18	75	36	123
Total	15806	19554	7757	22820	4504	889	5323	1123	1199	1036	7901

Figure 2: Vulnerable by types Common Vulnerabilities and Exposures (CVE) (http://www.cvedetails.com)

Year	Code Execution	Bypass	Privilege Escalation	Denial of Service	Information Leak
2014	1041	165	186	1597	356
2015	1430	177	255	1793	602
2016	1239	469	608	2050	704
2017	1870	857	1027	3372	1394
2018	1728	666	850	2207	1418
2019	1534	670	916	1699	1326
2020	1691	817	1387	1677	1094
2021	2087	806	1121	2297	926
2022	2067	943	1527	2437	1145
2023	2581	1059	1525	2559	1545
2024	469	235	248	498	200
Total	17737	6864	9650	22186	10710

Figure 3: Vulnerable by Impart Common Vulnerabilities and Exposures (CVE) (http://www.cvedetails.com)

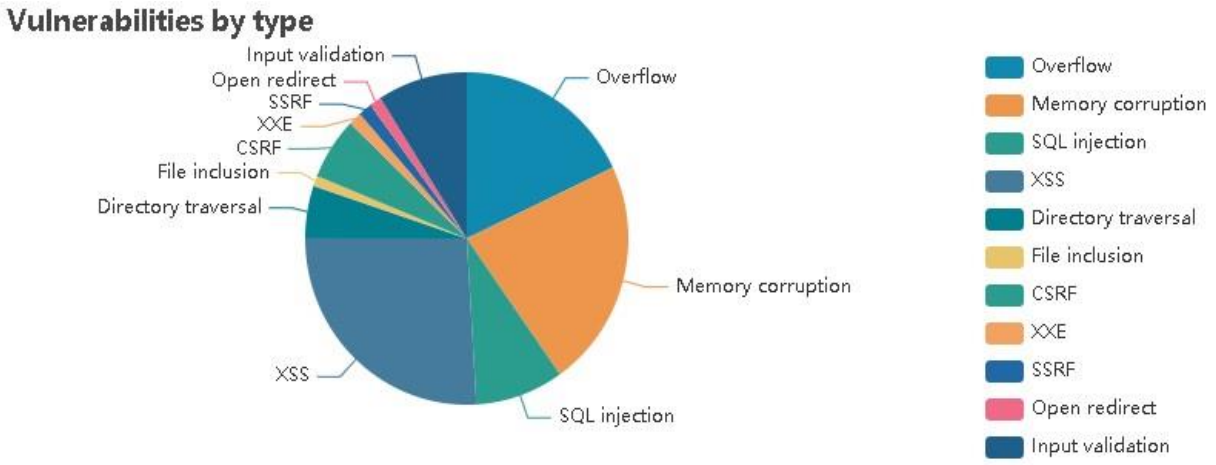

Figure 4: Vulnerable by Types Common Vulnerabilities and Exposures (CVE) website (http://www.cvedetails.com)

3. Results and Discussions

The results for this study are based on the research questions mentioned in the methodology. For RQ 1, which is about how vulnerable are IoT devices in smart cities to cyber-attacks, and what are the most common attack vectors. Rather than using an automated method like keyword search, the vulnerabilities discovered for IoT devices were identified by reading the vulnerability description. In 2023, there were a total of 24,848 vulnerabilities as presented in Figure 5. These vulnerabilities were further classified into 16 groups such as DoS, code execution etc.

	# of total Vulnerabilities	# of 16 types vulnerabilities	Privilege Escalation	Information leaks	Bypass	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	File inclusion	CSRF	XXE	SSRF	Open redirect	Input validation
Total	24848	24848	1525	1545	1059	2559	2581	1725	2813	2159	5179	808	137	1398	138	248	188	786
IoT device vulnerabilities	3530	3530	392	123	105	446	274	186	391	365	576	74	58	186	75	64	61	154
ratio of IoT devices vulnerabilities	14.20 %	14.20 %	25.70 %	7.90 %	9.90 %	17.40 %	10.60 %	10.80 %	13.90 %	16.90 %	11.10 %	9.10 %	42.30 %	13.30 %	10.80 %	25.80 %	32.40 %	19.60 %

Figure 5: Vulnerabilities of IoT devices.

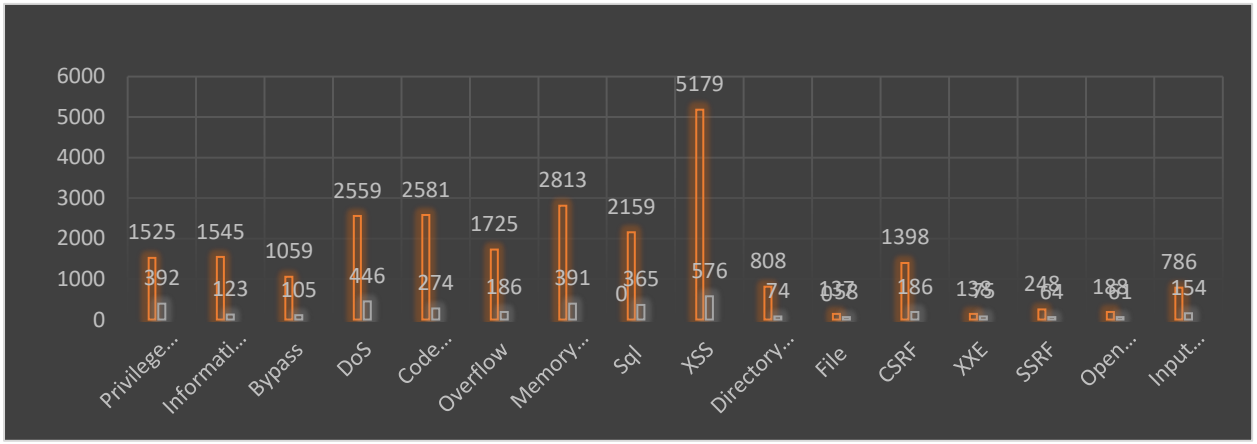

Figure 6: Number of Vulnerabilities of IoT devices.

Out of the 2,559 vulnerabilities as a result of DoS, 446 as shown in Figure 6 were discovered to be present in IoT devices while 274 IoT devices were determined to have code execution vulnerabilities out of the 2,581 in total. Figure 6 shows the number of each vulnerability. Figure 5 shows that in 2023, 13.9% of memory corruption vulnerabilities that were discovered were related to IoT devices. Among XSS vulnerabilities, IoT device vulnerabilities accounted for 11.10%, overflow vulnerabilities for 10.8%, DoS vulnerabilities for 17.4%, and bypass vulnerabilities for 9.9%. Open redirect, SQL injection vulnerability, information leak vulnerability, and privilege escalation vulnerability were 10.6%, 32.4%, 16.90%, 7.9%, and 25.70%, respectively.

With regards to RQ 2, concerned with what security and risk challenges of the data collected by IoT devices in smart cities are and how they can be addressed. During a careful study to address these RQ several concerns were identified. The following section addresses these concerns individually and also provided a mitigation strategy.

3.1 Security Concerns in Physical Layer

i. Unauthorized Access to Sensors and Other IoT Devices: Unauthorized access to sensors can be used by hackers to manipulate or manipulate the data collected. This can cause false readings or interrupt critical services. Unnecessary open ports (such as open SSH or Telnet ports) Unsecured boot process Unsecured firmware Unsecured and obsolete components.
ii. Physical Tampering: With physical access to sensors, attackers may be able to directly manipulate the hardware, compromising the quality of the data collected. Without a secure boot, IoT devices are vulnerable to another type of attack. Secure boot is necessary to protect an operating system from attack or to install a boot loader into IoT devices.
iii. Sensor Spoofing: Attackers may try to imitate or imitate sensor signals, giving the IoT system false information and causing false decisions to be made.
iv. Eavesdropping: Sensors and other components can be hacked, potentially exposing sensitive information or manipulating communications.

3.2 Privacy Concerns in Physical Layer

i. Location Privacy: Many sensors collect data related to location, raising concerns about the privacy of individuals and their movements.
ii. Biometric Data Collection: Sensors that capture biometric data for various purposes may infringe on privacy rights if not handled securely and responsibly.
iii. Data Aggregation: Aggregation of sensor data can result in the creation of detailed profiles, potentially revealing sensitive information about individuals or organizations.
iv. Ownership and Control: Ownership and control: determining the ownership and control of sensor data especially in shared environments, can lead to privacy-related disputes.

The risks experienced are:

i. Data Falsification: Incorrect or manipulated data from sensors can lead to incorrect conclusions and decisions, posing risks to the reliability and functionality of the entire IoT system.
ii. Environmental Factors: Sensors are susceptible to environmental conditions (e.g., extreme temperatures, humidity, electromagnetic interference) that may affect their accuracy and reliability.
iii. Scalability Challenges: Managing a large number of sensors in a scalable manner may pose challenges, potentially leading to gaps in security oversight.
iv. Resource Constraints: Resource-constrained sensors may lack the capability to implement robust security measures, making them more susceptible to attacks.

The possible mitigation strategies are:

i. Encryption: Implement encryption for communication between sensors and other components to protect data in transit.
ii. Mechanisms for Tamper Detection: Include systems that can identify physical tampering and sound an alarm when illegal access is discovered.
iii. Robust Authentication and Access constraints: To ensure that only authorized entities are able to connect with sensors, implement strong authentication and access constraints.

iv. Secure Protocols: Make use of secure communication protocols to guard against prying eyes and guarantee the accuracy of data transferred between sensors and the system as a whole.
v. Environmental Protections: Include environmental safeguards in sensor design to guarantee dependability under a range of circumstances.
vi. Privacy Impact Assessments: To identify and resolve any possible privacy issues related to sensor data, conduct privacy impact assessments.

3.3 Security Concerns in Network Layer

i. Man-in-the-Middle Attacks: These attacks enable data modification or unauthorized access by intercepting and manipulating data between Internet of Things devices and their connection endpoints.
ii. Eavesdropping: Insecure communication routes are vulnerable to eavesdropping, which gives hackers access to private data sent between devices.
iii. Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks: Networks connected to the Internet of Things (IoT) are vulnerable to disruptive assaults that might overwhelm communication channels, impairing the functionality of devices and services.
iv. Network Spoofing: Attackers may try to pose as genuine devices or fabricate phone network nodes, allowing for unauthorized access or data manipulation.

The risks experienced are:

i. Interference and Signal Jamming: Physical layer assaults that affect the dependability and accessibility of services might interfere with communication between Internet of Things devices. S
ii. Scalability Challenges: Managing the network infrastructure gets increasingly difficult as the number of IoT devices rises. Performance problems and heightened vulnerability might result from inadequate scalability.
iii. Insecure Protocols: Attackers may be able to take advantage of vulnerabilities at the network layer by using insecure communication protocols.
v. Traffic Analysis: Sensitive information can be deduced from patterns in data transfer, jeopardizing user security and privacy.

3.4 Privacy Concerns in Network Layer

i. Location Tracking: Device location information is frequently included in network layer data. User privacy may be violated by improper management of this data or by unauthorized access.
ii. Data Aggregation: Combining information from several Internet of Things devices might lead to the development of thorough user profiles, which raises questions around monitoring and possible abuse of the combined data.
iii. Metadata Exposure: Even if the content of the communication is encrypted, metadata (e.g., source, destination, timestamp) can still be exposed, providing insights into user behavior and habits.

The possible mitigation strategies are:

i. Reliable and Secure Communication Protocols: Use trustworthy and secure communication protocols, such as TLS (Transport Layer Security), to encrypt data in transit and prevent eavesdropping.

ii. Installing Intrusion Detection and Prevention Systems (IDPS) enables the monitoring of network activity, the detection of abnormalities, and the prevention of unauthorized access.
iii. Network Segmentation: To prevent potential security gaps, limit the impact of attacks, and improve network security generally, divide the Internet of Things network into parts.
iv. iv. Scalable architecture: Ensure that your current network architecture can accommodate the increasing quantity of IoT devices while maintaining security and speed. Firmware and Software Updates: Keeping up with regular firmware and software updates improves the security of devices linked to networks by addressing known vulnerabilities.
v. Privacy-Maintaining Strategies: Use strategies like differential firmware and software updates. Software and firmware updates help to improve the security of devices connected to networks by patching known vulnerabilities.
vi. Techniques for Preserving Privacy: To protect user privacy while retaining the capacity to do perceptive analysis, employ techniques like data anonymization and differential privacy.
vii. Transparency and User Consent: Users should be informed about data collecting procedures, given the opportunity to offer consent, and given the means to manage their privacy settings.

3.5 Security Concerns in Application Layer

i. Data Breaches: The application layer often handles sensitive information. If compromised, it can lead to unauthorized access, exposing personal or confidential data
ii. Unauthorized Access: Inadequate access restrictions or weak authentication methods might allow unauthorized users to take control of Internet of Things devices, potentially leading to abuse.
iii. Malware and Ransomware: Attacks utilizing malware and ransomware can affect Internet of Things (IoT) devices at the application layer, leading to outages, unauthorized access, or data encryption.
iv. Insecure APIs: Device communication is facilitated by Application Programming Interfaces, or APIs. It is possible to use insecure APIs to gain unauthorized access to or manipulate data.

The risks experienced are:

i. Interoperability Issues: The diverse range of IoT devices in smart cities may have varying standards and protocols, leading to interoperability challenges. This can create opportunities for attackers to exploit vulnerabilities arising from integration issues
ii. Denial of Service (DoS) Attacks: Application layer services can be targeted in DoS attacks, causing disruptions and preventing access to critical services
iii. Supply Chain Attacks: In a smart city ecosystem, devices often come from different manufacturers. A compromise in the supply chain can introduce malicious components, leading to security breaches
iv. Firmware and Software Vulnerabilities: Attackers can use outdated or insecure firmware and software in IoT devices to compromise the system as a whole.

3.6 Privacy Concerns in Application Layer

i. Surveillance and Tracking: IoT devices in smart cities may collect extensive data, raising concerns about citizen surveillance and tracking. Unauthorized access to this data can compromise privacy.
ii. Data Ownership and Consent: Determining ownership and obtaining user consent for the collection and use of data is often challenging. Lack of transparency in data practices can erode trust and violate privacy rights.
iii. Profiling and Analytics: The analysis of collected data for profiling and analytics purposes can lead to privacy infringements if not conducted responsibly and with proper safeguards.
iv. Location Tracking: Many IoT devices capture location data. Inappropriate use or disclosure of this information can lead to privacy violations and potentially compromise personal safety.

The possible mitigation strategies are:

i. Secure Development Practices: Conduct regular security audits of programmes and adhere to secure coding standards.
ii. Strong Encryption: To protect data both in transit and at rest, use strong encryption techniques.
iii. Authentication and Authorization: To ensure that only approved businesses may access IoT devices, establish strict authentication and authorization procedures. Regular updates and patch management: Updates for software and firmware fix known vulnerabilities.
iv. Privacy by Design: To reduce risks, incorporate privacy concerns from the outset of the creation of IoT devices.
v. Openness and Instruction for Users: Give them concise information about data practices and teach them how to keep their devices safe.

4. Conclusion and Recommendations

From several studied considered, it was observed that IoT technology has enormous potential to raise living standards and efficiency in smart cities. Realizing these advantages in a sustainable and responsible manner requires addressing security, privacy, and other related issues. Ongoing research and collaborative efforts are vitally important to successfully minimize these issues, which include the vulnerabilities that exist in IoT devices in smart cities as a result of things like weak authentication procedures, insufficient encryption, and poor device management methods. The increasing usage of IoT devices, which usually collect enormous volumes of personal data, including location, behavior patterns, and biometric data, raises privacy issues. If these data are not adequately safeguarded, they may be misused. Furthermore, supply chain hazards might be brought about by the inclusion of malicious components or by using firmware or software that is out of date and has not been patched. It is critical to address security, privacy, and related issues connected with IoT devices as smart cities continue to develop. Policymakers, urban planners, and technology players may reduce risks and guarantee that Smart City programmes put residents' rights and well-being first by putting in place comprehensive security measures, privacy-enhancing technologies, and strong regulatory frameworks. In order to promote innovation and preserve urban resilience as well as public trust in the digital age, efforts to protect IoT installations must be continuous and cooperative.

4.1 Challenges and Recommendations

For further studies, there are several potential areas that are crucial to ensuring sustainable and safe deployment of IoT devices for the development of urban environments. The potential areas are:

i. Threat Modeling and Risk Assessment: Develop comprehensive threat models and risk assessment frameworks specific to IoT deployments in smart cities.
ii. Technologies for Preserving Privacy: Investigate cutting-edge methods for decentralized identity management systems. for protecting user privacy and enabling the gathering and processing of data from Internet of Things devices.
iii. Block chain for IoT Security: Consider how block chain technology may improve security and confidence in IoT installations.
iv. Edge Computing Security: Research security issues and remedies unique to edge computing architectures that are frequently employed in smart city settings.
v. Human-Centric Security Solutions: Examine how user behavior, knowledge, and risk perception are human variables that impact the security and privacy of IoT devices in smart cities.
vi. Disaster Recovery and Resilience: Look on ways to make smart city infrastructure more resilient to both natural catastrophes and cyber-physical threats.

References

[1] Rao, Patruni & Deebak, Dr. B. D.. (2022). Security and privacy issues in smart cities/industries: technologies, applications, and challenges. Journal of Ambient Intelligence and Humanized Computing. 14. 1-37. 10.1007/s12652-022-03707-1.

[2] Siman, Emmanuel & Abiodun, John & Timothy, Gani & Nandom, Sumayyah. (2023). IoT-Driven Smart Cities: Enhancing Urban Sustainability and Quality of Life.

[3] Gasim Alandjani, (2018) "Features and Potential Security Challenges for IoT Enabled Devices in Smart City Environment" International Journal of Advanced Computer Science and Applications(ijacsa), 9(8), 2018. http://dx.doi.org/10.14569/IJACSA.2018.090830

[4] Hassebo, Ahmed, and Mohamed Tealab. (2023). "Global Models of Smart Cities and Potential IoT Applications: A Review" *IoT* 4, no. 3: 366-411. https://doi.org/10.3390/iot4030017

[5] Fabrègue, Brian F. G., and Andrea Bogoni. 2023. "Privacy and Security Concerns in the Smart City" *Smart Cities* 6, no. 1: 586-613. https://doi.org/10.3390/smartcities6010027

[6] Antonopoulos, K., Petropoulos, C., Antonopoulos, C. P., & Voros, N. S. (2017). Security data management process and its impact on smart cities' wireless sensor networks. Paper presented at the South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference, SEEDA-CECNSM 2017, https://doi.org/10.23919/SEEDA-CECNSM.2017.8088238.

[6] Elmaghraby, A. S., & Losavio, M. M. (2014). Cyber security challenges in smart cities: Safety, security and privacy. *Journal of Advanced Research, 5*(4), 491–497. https://doi.org/10.1016/j.jare.2014.02.006.

[7] R. Chawla, et al., (2021) Study of security threats and challenges in Internet of things systems, Turkish Journal of Computer and Mathematics Education (TURCOMAT) 12 (2) (2021) 1154–1166.

[8] Ainane, N., Ouzzif, M., & Bouragba, K. (2018). Data security of smart cities. Paper presented at the ACM International Conference Proceeding Series, https://doi.org/10.1145/3286606.3286866.

[9] Alandjani, G. (2018). Features and potential security challenges for IoT-enabled devices in smart city environment. *International Journal of Advanced Computer Science and Applications, =rx n9*(8), 231–238.

[10] Khando, Shang Gao, Sirajul M. Islam, Ali Salman (2021), Enhancing employees information security awareness in private and public organisations: A systematic literature review, Computers & Security, Volume 106, 102267, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2021.102267.

[11] Hyesoo Jeon, Changjun Lee, (2022), Internet of Things Technology: Balancing privacy concerns with convenience, Telematics and Informatics, Volume 70, 101816, ISSN 0736-5853, https://doi.org/10.1016/j.tele.2022.101816.

[12] Porambage P., Ylianttila M., Schmitt C., Kumar P., Gurtov A., Vasilakos A. V. (2016). The quest for privacy in the Internet of Things. *IEEE Cloud Comput.* 3, 36–45. 10.1109/MCC.2016.28

[13] Yang G.(2022) An Overview of Current Solutions for Privacy in the Internet of Things. Front Artif Intell. Mar 3;5:812732. doi: 10.3389/frai.2022.812732. PMID: 35310954; PMCID: PMC8928167.

[14] R. Kitchin (2014), The real-time city? Big Data and Smart Urbanism GeoJournal, 79 (1), pp. 1-14

[15] P. Neirotti, A. De Marco, A.C. Cagliano, G. Mangano, F. Scorrano (2014) Current trends in Smart City initiatives: Some stylised facts Cities, 38, pp. 25-36

[16] Chiehyeon Lim, Kwang-Jae Kim, Paul P. Maglio, (2018), Smart cities with big data: Reference models, challenges, and considerations, Cities, Volume 82, Pages 86-99, ISSN 0264-2751, https://doi.org/10.1016/j.cities.2018.04.011.

[17] Shahbaz Pervez, Nasser Abosaq, Gasim Alandjani, Adeel Akram, (2018)"Internet of Things (IoT) as Beginning for Jail-Less Community in Smart Society", "IEEE International Conference on Electrical, Electronics, Computers, Communication, Mechanical and Computing 28-29 January 2018 at Tamil Nado India.

[18] Li, Shancang & Tryfonas, Theo & Li, Honglei. (2016). The Internet of Things: a security point of view. Internet Research. 26. 337-359. 10.1108/IntR-07-2014-0173.

[19] Hyesoo Jeon, Changjun Lee, (2022), Internet of Things Technology: Balancing privacy concerns with convenience, Telematics and Informatics, Volume 70, 101816, ISSN 0736-5853, https://doi.org/10.1016/j.tele.2022.101816.

[20] Golightly L, Chang V, Xu QA, Gao X, Liu BS. Adoption of cloud computing as innovation in the organization. International Journal of Engineering Business Management. 2022;14. doi:10.1177/18479790221093992 locations and Computing. 12. 1-33. 10.4018/IJCAC.308277.

[21] Sun Y, Zhang J, Xiong Y, Zhu G. Data Security and Privacy in Cloud Computing. International Journal of Distributed Sensor Networks. 2014;10(7). doi:10.1155/2014/190903

[22] Jawed, Md Saquib & Sajid, Mohammad. (2022). A Comprehensive Survey on Cloud Computing: Architecture, Tools, Technologies, and Open Issues. International Journal of Cloud App 1.

[23] Trevor Braun, Benjamin C.M. Fung, Farkhund Iqbal, Babar Shah, (2018), Security and privacy challenges in smart cities, Sustainable Cities and Society, Volume 39, Pages 499-507, ISSN 2210-6707, https://doi.org/10.1016/j.scs.2018.02.039.

[24] Rao, Patruni & Deebak, Dr. B. D.. (2022). Security and privacy issues in smart cities/industries: technologies, applications, and challenges. Journal of Ambient Intelligence and Humanized Computing. 14. 1-37. 10.1007/s12652-022-03707-1.

[25] Ismagilova, Elvira & Hughes, Laurie & Rana, Nripendra & Dwivedi, Yogesh. (2022). Security, Privacy and Risks Within Smart Cities: Literature Review and Development of a Smart City Interaction Framework. Information Systems Frontiers. 24. 10.1007/s10796-020-10044-1.

[26] Majid, A. (2023) Security and Privacy Concerns over IoT Devices Attacks in Smart Cities (2022). *Journal of Computer and Communications*, **11**, 26-42. doi 10.4236/jcc.2023.111003.

[27] Bagga, P., Das, A.K., Wazid, M., Rodrigues, J.J., Choo, K.K.R. and Park, Y. (2021) On the Design of Mutual Authentication and Key Agreement Protocol in Internet of Vehicles-Enabled Intelligent Transportation System. IEEE Transactions on Vehicular Technology, 70, 1736-1751.

[28] Davis, B.D., Mason, J.C. and Anwar, M. (2020) Vulnerability Studies and Security Postures of IoT Devices: A Smart Home Case Study. IEEE Internet of Things Journal, 7, 10102-10110. https://doi.org/10.1109/JIOT.2020.2983983

[29] Görmüş, S., Aydın, H. and Ulutaş, G. (2018) Security for the Internet of Things: A Survey of Existing Mechanisms, Protocols and Open Research Issues. Journal of the Faculty of Engineering and Architecture of Gazi University, 33, 1247-1272.

[30] Ahmed, Saleem. (2020). Security and Privacy in Smart Cities: Challenges and Opportunities. International Journal of Engineering Trends and Technology. 68. 1-8. 10.14445/22315381/IJETT-V68I2P201.

[31] Cui, Lei & xie, gang & Qu, Youyang & Gao, Longxiang & yang, yunyun. (2018). Security and Privacy in Smart Cities: Challenges and Opportunities. IEEE Access. PP. 1-1. 10.1109/ACCESS.2018.2853985.

[32] Al-Turjman F, Zahmatkesh H, Shahroze R. An overview of security and privacy in smart cities' IoT communications. Trans Emerging Tel Tech. 2019; e3677. https://doi.org/10.1002/ett.3677

[33] Sookhak, Mehdi & Yu, F. & Tang, Helen. (2018). Security and Privacy of Smart Cities: A Survey, Research Issues and Challenges. IEEE Communications Surveys & Tutorials. PP. 10.1109/COMST.2018.2867288.

[34] Ismagilova, E., Hughes, L., Rana, N.P. et al. Security, Privacy and Risks Within Smart Cities: Literature Review and Development of a Smart City Interaction Framework. Inf Syst Front 24, 393–414 (2022). https://doi.org/10.1007/s10796-020-10044-1

[35] Pandya, H.B.; Champaneria, T.A. (2015) Internet of things: Survey and case studies. In proceedings of the 2015 International Conference on Electrical, Electronics, Signals, Communication and Optimization (EESCO), Visakhapatnam, India, 24–25 January 2015; pp. 1–6.

[36] McEwen, A.; Cassimally, H.(2014) *Designing the Internet of Things*; Wiley: Hoboken, NJ, USA, 2014.

[37] Bellini, Pierfrancesco, Paolo Nesi, and Gianni Pantaleo. (2022). "IoT-Enabled Smart Cities: A Review of Concepts, Frameworks and Key Technologies" Applied Sciences 12, no. 3: 1607. https://doi.org/10.3390/app12031607

[38] Syed, A.S.; Sierra-Sosa, D.; Kumar, A.; Elmaghraby,(2021) A. IoT in smart cities: A survey of technologies, practices and challenges. *Smart Cities, 4*, 24. Pukkasenung, P.; Lilakiatsakun, W. Improved generic layer model for IoT architecture. *J. Inf. Sci. Technol.* 2021, *11*, 18–29.

[39] Said, O.; Masud, M.(2013) Towards the Internet of Things: Survey and future vision. *Int. J. Comput. Netw.* , *5*, 1–17.

[40] Zhong, C.-L.; Zhu, Z.; Huang, R.-G.(2015) Study on the IoT architecture and gateway technology. In Proceedings of the 14th International Symposium on Distributed Computing and Applications for Business Engineering and Science, Guiyang, China, 18–24 August 2015.

[41] Burhan, M.; Rehman, R.A.; Khan, B.; Kim, B.S. (2018) IoT elements, layered architectures and security issues: A comprehensive survey. *Sensors*, *18*, 2796.

[42] Marques, G.; Garcia, N.; Pombo, N. (2017)A survey on IoT: Architectures, elements, applications, QoS, platforms and security concepts. In *Advances in Mobile Cloud* Computing and Big Data in the 5G Era; Springer: Cham, Switzerland, pp. 115–130.

[43] Tekinerdogan, Bedir, Ömer Köksal, and Turgay Çelik. (2023). "System Architecture Design of IoT-Based Smart Cities" Applied Sciences 13, no. 7: 4173. https://doi.org/10.3390/app13074173

[44] Al-Masri, Eyhab & Kalyanam, Karan & Batts, John & Kim, Jonathan & Singh, Sharanjit & Vo, Tammy & Yan, Charlotte. (2020). Investigating Messaging Protocols for the Internet of Things (IoT). IEEE Access. PP. 1-1. 10.1109/ACCESS.2020.2993363.

[45] S. Al-Sarawi, M. Anbar, K. Alieyan, and M. Alzubaidi,(2017) ‘‘Internet of Things (IoT) communication protocols: Review,’’ in Proc. 8th Int. Conf. Inf. Technol. (ICIT), May 2017, pp. 685–690.

[46] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, (2015)‘' Internet of Things: A survey on enabling technologies, protocols, and applications," IEEE Commun. Surveys Tuts., vol. 17, no. 4, pp. 2347–2376, 4th Quart., 2015.

[47] Bellini, Pierfrancesco, Paolo Nesi, and Gianni Pantaleo. 2022. "IoT-Enabled Smart Cities: A Review of Concepts, Frameworks and Key Technologies" Applied Sciences 12, no. 3: 1607. https://doi.org/10.3390/app12031607

[48] J. K. D. Barriga, C. D. G. Romero, and J. I. R. Molano,(2016). “Proposal of a standard architecture of IoT for smart cities," in International Workshop on Learning Technology for Education Challenges. Springer, 2016, pp. 77–89.

[49] Abawajy, J.; Darem, A.; Alhashmi, A.A. (2021) Feature subset selection for malware detection in smart IoT platforms. Sensors, 21, 1374.

[50] Mahdin, H.; Abawajy, J. (2011) An approach for removing redundant data from RFID data streams. Sensors, 11, 9863–9877.

[51] Afzaal R, Shoaib M. (2021) Data recoverability and estimation for perception layer in a semantic web of things. PLoS One. 2021 Feb 26;16(2):e0245847. doi: 10.1371/journal.pone.0245847. PMID: 33635878; PMCID: PMC7909669.

[52] Kasmi M., Bahloul F., Tkitek H.(2016) Smart home based on Internet of Things and cloud computing; Proceedings of the 7th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT); Hammamet, Tunisia. 18–20 December 2016; pp. 82–86.

[53] Ejaz W., Anpalagan A., Imran M.A., Jo M., Naeem M., Qaisar S.B., Wang W. Internet of Things (IoT) in 5G wireless communications. IEEE Access. 2016;4:10310–10314. doi: 10.1109/ACCESS.2016.2646120.

[54] Madakam S., Lake V., Lake V., Lake V. Internet of Things (IoT): A literature review. J. Comput. Commun. 2015;3:164. doi: 10.4236/jcc.2015.35021.

[55] O. Bello et al., (2016), Network layer inter-operation of Device-to-Device communication technologies in Internet of Things (IoT), Ad Hoc Networks (2016), http://dx.doi.org/10.1016/j.adhoc.2016.06.010

[56] Tomás Domínguez-Bolaño, Omar Campos, Valentín Barral, Carlos J. Escudero, José A. García-Naya, (2022). An overview of IoT architectures, technologies, and existing open-source projects, Internet of Things, Volume 20, 100626, ISSN 2542-6605, https://doi.org/10.1016/j.iot.2022.100626.

[57] Tariq, Usman, Irfan Ahmed, Ali Kashif Bashir, and Kamran Shaukat. (2023) "A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review" Sensors 23, no. 8: 4117. https://doi.org/10.3390/s23084117

[58] Somayeh Nasiri, Farahnaz Sadoughi, Afsaneh Dehnad, Mohammad Hesam Tadayon, Hossein Ahmadi(2021) Layered Architecture for Internet of Things-based Healthcare System: A Systematic Literature Review information 45 (2021) 543–562 543 https://doi.org/10.31449/inf.v45i4.3601.

[59] Baho, Samira A., and Jemal Abawajy. 2023. "Analysis of Consumer IoT Device Vulnerability Quantification Frameworks" Electronics 12, no. 5: 1176. https://doi.org/10.3390/electronics12051176

[60] Majid, A. (2023) Security and Privacy Concerns over IoT Devices Attacks in Smart Cities (2022). Journal of Computer and Communications, 11, 26-42. https://doi.org/10.4236/jcc.2023.111003.

[61] Vulnerabilities by type [Online]. Available: https://www.cvedetails.com/vulnerabilities-by-types.php.