A Study of Ways to Protect IoT Communication Networks from Penetration in Smart Cities

Mustafa, K. Ati

Abstract This study examines the problems of penetration and hacking of Internet of Things communications networks, explaining the types and methods of global hacking, and how to address these problems in light of the rapid development of communications networks for smart cities. It includes a comprehensive survey of methods of penetration and attack by enemies who want to obtain results that benefit them, such as people's confidential data. The important results were how to avoid these attacks as much as possible by following clear and important steps, and this is shown in Table I in this research.

***Index Terms*— Assault, IoT smart cities, Security**

I. INTRODUCTION

THE topic addressed by publicizing the dangers, weaknesses, and user behavior on open social networks in an effort to improve security and privacy while promoting community participation in smart cities. Furthermore, a new model that illustrates the relationships between security and privacy threats is proposed, along with a few practical defenses, to defend Wireless Sensor Networks (WSNs) users in smart cities [1]. The surge in the Internet of Things IoT will make Smart Cities (SCs) and Smart Homes (SHs) inevitable. Home Automation (HA) became possible as personal computers started to become a common sight in homes in the late 1970s thanks to enthusiasts. SH has long been an objective and is the core of smart cities [2]. WSNs' ad hoc network architecture allows for the communication of numerous low-power, multipurpose nodes with one another in the vicinity. WSNs are typically made up of inexpensive, low-capacity sensor devices because deployment costs are a major factor in Internet of Things applications. restricted processing and data transmission capacity [3]. The next big technical advance that will significantly improve many facets of the human environment, including business, transportation, and health, is the Internet of Things IoT. But even if it might result in positive social and economic developments, protecting users' and objects' privacy and security continues to be a major issue that needs to be resolved [4]. The interplay of "things" and gadgets, such as wearable's, sensors, actuators, mobile phones, computers, meters, and even cars, is an important aspect of the modern world. These interconnected networks promote the development of applications like as smart cities and infrastructure, smart industries, smart-everything, and home and building automation. But with no room for error, the security of these networked Internet of Things IoT plays a critical role. [5]. The Internet of Things era began with the goal of using the Internet to connect all digital and analog equipment worldwide via the software defined network (SDN) depicted in figure (1). According to predictions, billions of devices would need to be linked together by 2050 to provide enhanced, tailored services. A smart city, or an IT-enabled city that operates intelligently without human intervention, is one use for the Internet of Things [6]. As a result, most proposed solutions for secure routing and data collection protocols rely on Symmetric-Key cryptography, which introduces new security concerns. The impact of the Internet of Things vision on the various security criteria that should be studied in WSNs is something that has to be looked into to get a handle on the concerns and challenges related to Security in WSNs, It is called Part 2. The security requirements of a WSN and how they might be compromised must also be identified and described, along with the attacks and threats they may pose to the values of the network As in Section 3. Then, we'll go deep into the difficulty of securing the essential aspects of WSNs, including the aforementioned fundamental security vulnerabilities like in Section 4. Complete integration into

Mustafa, K. Ati is with Department of Electrical, Engineering & College of Engineering, University of Misan, Iraq. (Email: Mustafak302@uowasit.edu.iq)

ISSN: 2961-5992

IoT applications still has the hurdles to solving various security investigation difficulties, in contrast to the technical security problems of the WSN's which have been widely explored in past works.

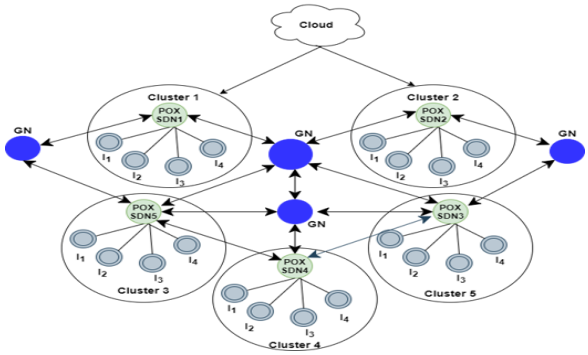

Fig. 1. Clustering in IoT for SDN Controller [6].

II. The Need for IoT Security in Wireless Sensor Networks

WSNs are becoming increasingly vital as technology advances, and sensors are already being used in a variety of settings. The limitations of WSNs are that they become exceedingly complex to use [7]. The Internet of Things IoT is rapidly expanding in the ICT industry [8], Security is an absolute must-have. Advantages like mobility and increased availability to massive installations are provided by WSNs that comply with the ad-hoc method [9]. As a result, it has legitimate potential as a long-term enabler of IoT deployments in fields including industrial monitoring, environmental monitoring, and healthcare monitoring. However, several problems need more widespread fixing (e.g. erratic communications, massive scale, and unattended operation) [10]. To meet the particular limits of WSNs, the security needs of the IoT can include not just the standards used in traditional networks but also those specific to these new types of devices. As a result, the large and small requirements [14] for investigating WSN's Security can be broken down as follows:

A. The Essential Prerequisites

The following are the primary standards, which are considered to be the standard security requirements:

1. The privacy of sending responsive sensed data must be protected from eavesdroppers, such as passive attackers, at all times. Feeling data should be kept private during collection and transmission. This can be achieved by encrypting the collected data using a key known only to the intended recipients [11].
2. Source Authentication: The ability to ensure the reliability of the collected and transmitted sensing data through the WSN's by verifying its source and data origin. Therefore, the communication turns out to be genuine since the malicious node cannot pretense in place of a trusted node. Consequently, Source Authentication is essential for decisions making and exchanging the control information of the WSN's [12].
3. Thirdly, we must ensure and verify the accuracy of the data we acquire. Even though the communication environment in WSNs can be challenging, data transmissions with in the networks have never been compromised.
4. It guarantees that the targeted WSNs are accessible for communication services and that all nodes can access the network's resources, even when DDoS attacks are present. Due to their central role in maintaining the connectivity of IoT devices, WSNs are crucial to the continued operation of IoT services and applications.

B. Minimal Prerequisites

1. Data is guaranteed to be as new as possible before being sent, which helps prevent replaying attacks on data transmission infrastructure. This is by assuring that such old information will not be replayed again. Thus, the communicated information will be recent [14], which can be achieved by introducing a moment timer into the transfer packet.
2. Every node in a WSN is autonomous and configurable, allowing the network to self-organize in response to changing conditions due to the decentralized nature of WSNs.
3. Data exchange is essential in many WSN uses for instance; the sensors' radios could be switched off at regular intervals to save power.
4. Safe Volunteers: The success of a WSN depends heavily on its ability to pinpoint the precise locations of each sensor node in the network. However, adversaries can trick unsecured location data by providing fabricated signal strengths or duplicating signals.

III. Strike & Vulnerabilities

Based on our application deployment, it is evident that typical smartphone application design methodologies would not be appropriate for a less tech-savvy target group. Indigenous and ethnic communities make up a small percentage of the large stakeholder groups in traditional software development. As a result, their needs and expectations are disregarded throughout the creation of smartphone applications. As a result, persons from minority ethnic groups lag behind when it comes to employing various digital interventions [14,15].

IV. Internet of Thing Connection Hurdles

The Home automation design is complicated, with billions of instruments and items interacting with one another and other elements such as humans or artificial entities [8]. Due to their affordability, effectiveness, and small size, wireless sensor networks WSNs have become an

ISSN: 2961-5992

essential part of the networking industry and are useful for a wide range of applications. However, these networks struggle with innate limits including memory and processing constraints as the reliance on WSN-dependent applications grows. Consequently, timely attention is needed for effective solutions, particularly in the era of the Internet of Things IoT, which heavily depends on WSN efficacy. Various heterogeneous objects appear in different contexts, and connecting contributes to the IoT's complexity, further complicating network security deployment [20].

A. Security Issues

Wireless Sensor Networks WSNs and the Internet of Things IoT are developing in the current digital era, changing human experiences through the creation of an interconnected world. But maintaining the security of WSN-IoT networks continues to be a major challenge because current security models have problems with things like lengthy training times and intricate classification procedures [21]. However, employing encryption as a security measure is insufficient to preserve data and information security. The eavesdropped cipher data can be analyzed for traffic, allowing the attacker to decrypt and reveal sensitive information. When a malicious node is infiltrated as one communication terminal, sensitive data and information may be leaked, thus compounding the secrecy difficulties. Moreover, the attacker node can successfully exploit the radio frequency range of other edge devices when using a group shared key, allowing it to eavesdrop on and decrypt the private data and information being transmitted.

B. Difficulties in Verifying Reliable Sources

In typical sensor networks, attackers not only modify existing communication packets but also inject new, fraudulent packets as part of their attacks [14]. Authenticating data in WSNs is difficult since they operate in unsupervised settings and over a public wireless network. To enable sensor nodes to tell the difference between vindictively injected and phishers packets and the original packets from the legitimate source, source authentication can be attained through symmetric and asymmetric processes, where the transmission and reception nodes share private keys to confirm the resource identity [13]. It's clear from the numbers that To access the protected areas of most applications, In the case of military and protection applications, for instance, it is easy to see why attackers would try to compromise sensor nodes by inserting bogus data reports or redirecting traffic. Even in what may be considered a more peaceful setting, such as a civilian application, data loss is a real possibility without proper identification. When a node is compromised, it may still identify itself in the network by obtaining the encryption key from the legitimate nodes. Hence data authentication does not solve the node compromise problem. However, the hacked nodes in the network can be identified and their encryption secret keys revoked using intrusion detection techniques.

C. Difficulties in Maintaining Data Security

Organizations can benefit from cloud-based data storage solutions in a number of ways, such as easier IT infrastructure and management, remote access from virtually anywhere in the world with a reliable Internet connection, and cost savings from cloud computing. However, there are security and privacy issues related to cloud computing that need to be further investigated. In earlier studies, researchers from industry, academia, and standards organizations have offered some potential solutions [14] figure (2). For instance, rogue nodes may alter the contents of communication packets or inject bogus data. In that case, the WSN's base station will somehow receive packages that have been changed. However, the hostile communication environment may lead to data loss or corruption without a rogue node. Therefore, it is crucial to maintain data integrity when transmitting information within WSNs to avoid the possibility of data corruption or loss.

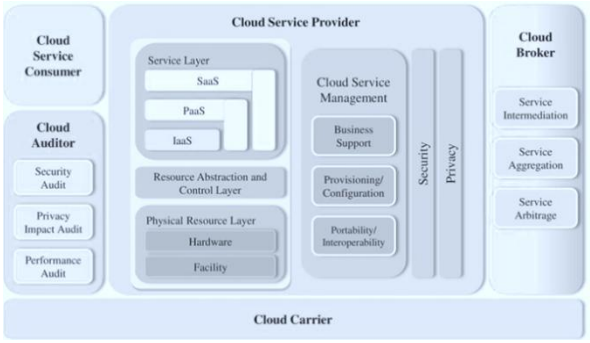

Fig. 2 Cloud Computing Configuration [14]

D. Impact the Jamming on the connection

Because of their limited features and capabilities, Internet of things IoT devices are vulnerable to a variety of safety concerns. Wireless communications between power-limited nodes in the Internet of Things are typically shown sporadically. It is possible to grab IoT devices and launch a node repetition assault, for example. An effective, exact, and rash recognition technique that can identify jammers and replicated nodes in the network is essential for wireless sensor networks WSNs [13]. Costs rise when traditional encryption methods need to be modified to meet the needs of WSN security. Some of the techniques mentioned in the literature involve extensively changing and reusing existing code. Other ways of accomplishing the same thing typically involved more extensive use of communications channels. Moreover, several methods place stringent constraints on the data that may be accessed or provide subpar schemes (like the central point scheme) to speed up the procedure.

ISSN: 2961-5992

Therefore, availability is crucial for ensuring the continued functioning of WSN's operational services and the network.

V. CONCLUSION

With a brief overview and threat of external attacks to networks and security requirements detailed and precise in Table No. (1). In regard to this line of research, there is still a significant amount of territory to cover. To be more specific, this will be the case when it comes to resolving the most pressing security issues that the future IoT service will face. This can be done by developing a universal, all-encompassing platform that enables instantaneous, global, ubiquitous communication between anything and everything.

REFERENCES

[1] Kusumastuti, Ratih Dyah, et al. "Analyzing the factors that influence the seeking and sharing of information on the smart city digital platform: Empirical evidence from Indonesia." Technology in Society 68 (2022): 101876.

[2] Yershova, O. L., and L. I. Bazhan. "Smart city: concept, models, technologies, standardization." Statistics of Ukraine 8990.2-3 (2020): 68-77.

[3] Al-Quayed, Fatima, Zulfiqar Ahmad, and Mamoona Humayun. "A situation based predictive approach for cybersecurity intrusion detection and prevention using machine learning and deep learning algorithms in wireless sensor networks of industry 4.0." IEEE Access (2024).

[4] Srivastava, Animesh, and Anoop Kumar. "Secure Authentication Scheme for the Internet of Things." International Journal on Recent and Innovation Trends in Computing and Communication 11.4s (2023): 182-192.

[5] Aouedi, Ons, et al. "A survey on intelligent Internet of Things: applications, security, privacy, and future directions." IEEE Communications Surveys & Tutorials (2024).

[6] Babbar, Himanshi, et al. "Cloud based smart city services for industrial internet of things in software-defined networking." Sustainability 13.16 (2021): 8910.

[7] Ibrahim, Dheyab Salman, Abdullah Farhan Mahdi, and Qahtan M. Yas. "Challenges and issues for wireless sensor networks: A survey." J. Glob. Sci. Res 6.1 (2021): 1079-1097. 34

[8] Worlu, Chijioke, Azrul Amri Jamal, and Nor Aida Mahiddin. "Wireless sensor networks, internet of things, and their challenges." International Journal of Innovative Technology and Exploring Engineering 8.12S2 (2019): 556-566.

[9] Burhanuddin, M. A., et al. "A review on security challenges and features in wireless sensor networks: IoT perspective." Journal of Telecommunication, Electronic and Computer Engineering (JTEC) 10.1-7(2018):17-21.

[10] Ahmed, Hassan I., et al. "A survey of IoT security threats and defenses." International Journal of Advanced ComputerResearch9.45(2019):325-350.

[11] JAYABALAJI, KA, and A. MUTHUCHUDAR. "Enhancing the Stability of Underwater Wireless Sensor Networks Using Firefly Swarm Intelligence Approach." International Journal of Modern Agriculture10.1(2021):1005-1013.

[12] Xu, Weitao, et al. "Key generation for Internet of Things: a contemporary survey." ACM Computing Surveys (CSUR)54.1(2021):1-37.

[13] Jeyaselvi, M., et al. "SVM-Based Cloning and Jamming Attack Detection in IoT Sensor Networks." Advances in Information Communication Technology and Computing: Proceedings of AICTC 2021. Singapore: Springer Nature Singapore, 2022. 461-471.

[14] Tabrizchi, Hamed, and Marjan Kuchaki Rafsanjani. "A survey on security challenges in cloud computing: issues, threats, and solutions." The journal of supercomputing 76.12 (2020): 9493-9532.

[15] Rajawat, Anand Singh, et al. "Vulnerability analysis at industrial internet of things platform on dark web network using computational intelligence." Computationally intelligent systems and their applications (2021): 39-51.

[16] Bugeja, Joseph. "On privacy and security in smart connected homes." (2021).

[17] Walters, John Paul, et al. "Wireless sensor network security: A survey." Security in distributed, grid, and pervasive computing (2006):208-222.

[18] Alaba, Fadele Ayotunde, et al. "Internet of Things security: A survey." Journal of Network and Computer Applications88(2017):10-28.

[19] Hasan, Muhammad Zulkifl, Zurina Mohd Hanapi, and Muhammad Zunnurain Hussain. "Wireless Sensor Security Issues on Data Link Layer: A Survey." Computers, Materials & Continua 75.2 (2023).

[20] Mushtaq, Muhammad Umer, et al. "Enhancing Security and Energy Efficiency in Wireless Sensor Network Routing with IOT Challenges: A Thorough Review." LC International Journal of STEM (ISSN: 2708-7123) 4.3 (2023): 1-24.

[21] Krishnasamy, Sundaramoorthy, et al. "Development and Validation of a Cyber-Physical System Leveraging EFDPN for Enhanced WSN-IoT Network Security." Sensors 23.22 (2023): 9294.G. O. Young, "Synthetic structure of industrial plastics (Book style with paper title and editor)," in *Plastics*, 2nd ed. vol. 3, J. Peters, Ed. New York: McGraw-Hill, 1964, pp. 15–64.

ISSN: 2961-5992

TABLE I
REAL THREAT ASSESSMENT

Safety Prerequisites	Threats	Brief overview
The integrity of Authenticity and Privacy	Strike of duplication nodes	Adding copies of valid nodes to a present WSN [15] allows for communication with the communication link from the duplicated node [16].
	Threats to confidentiality Listening in and spying passively on others	Without a robust cryptographic method, opponents can easily eavesdrop on unsecured WSN transmissions and decipher their components [17].
	Strike on network monitoring	The adversary can identify nodes with specialized responsibilities or occupations, which may offer critical data about the network's broadcasting [17].
	Strike in disguise	When an attacker inserts destructive intermediary terminals into WSNs, the attack is said to be [11]. Once inside the intended WSNs, these nodes can be exploited to trick communication packets into thinking they are being sent to a trusted node by broadcasting fake routing information.
Authenticity of Performance	Sneaky strikes	Threat actors can launch covert strikes on the reliability of a WSN's services. The enemy uses Shadow assaults to trick WSNs into believing fabricated information.
Types Of attacks: When a Server Is Unavailable	Physical Layer, Assault via interference Tampering attack	Attack the legal radio frequencies used by WSN nodes [15]-[18]. Extraction of data from nodes in a WSN, including data encryption and other sensitive information, via physical access [18].
	The data Link Layer, Congestion assault	When multiple nodes are transmitting in every spectral region simultaneously, interference occurs.
	Saturation assault	Industry trends indicate that many ISPs are looking at Layer 2 (L2) services for the last mile to the customer[19].
	Unfair criticism assault	Use the aforementioned link-layer attacks on WSNs unfairly and sporadically.

ISSN: 2961-5992