j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 6 , special issue 2023

Developing Smart City security through Upgrade Internet of Things Layers security

Wasan A. Al-Hamami[1] , Mazin S. Al-Hakeem[2], Alaa H. Al-Hamami[3]

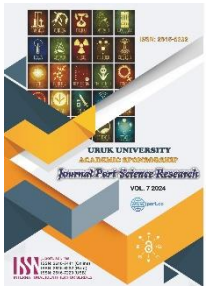
[1]*Informatics Institute for Postgraduate Studies.*

[2]*Al Hikma University College, Baghdad, Iraq.*

[3] *Alshaab University College, Baghdad, Iraq*

an_alhamami@yahoo.com

Abstract Lot devices like connected sensors, lighting, and meters are used in smart cities to collect and analyze data. The cities utilize this information to enhance their infrastructure, public services, and more. A public/private infrastructure must be established in order to execute operations and supply the technologies necessary to protect and secure citizens in order to maintain a secure smart safe city. This contains the following three essential actions: 1) Shared intelligence, communications, and situational awareness. The Internet of Things (IoT) is essentially a network that connects electronic gadgets to the internet, enabling seamless network communication between them. Security is an important issue in the IoT environment, where the protection of data is an urgent process. Every object will be connected to the internet and these objects communicate between each other. Therefore, a new security and privacy problems will appear. This paper introduces several security concepts on each IoT layer. Additionally, illustrates the security goals, challenges and security methods in each layer. Finally, this paper will develop a secure Smart city through improving the IoT layers security.



10.36371/port.2023.special.6

Keywords: *Smart City, IOT, Security, challenges, integrity, confidentiality, availability, threats.*

1. INTRODUCTION

Critical Infrastructure use Supervisory Control and Data Acquisition (SCADA) systems for monitoring and remote control. Sensor networks are been integrated into all areas of the infrastructures of smart cities. The sensor network data stream contains information that can be utilized to model and control the activity of these infrastructures. This paper primary's objective is to explain and suggest methods to detect hostile intrusions and solve the challenges that faced the Internet of Things (IoT). In recent decades, sensor network has monitored and controlled a significant portion of smart cities' critical infrastructure. These infrastructures consist of IoT' devices, Sewage treatment facilities, air conditioning units, railroads, a water network, and power stations.

Information and communication technology (ICT) is used in smart cities to increase operational effectiveness, disseminate information to the general public, and improve the quality of public services and citizen welfare. By utilizing smart technologies and data analysis, a smart city aims to improve citizen quality of life, enhance city operations, and foster economic growth. Instead of just how much tech is accessible, the value is in how it is used. A city's smartness is determined using a set of characteristics, including:

a) A technologically based infrastructure.
b) Environmentally friendly programs.
c) A well-functioning and efficient public transit system.
d) d. Promising and forward-thinking city ideas.
e) People who can live and work in the city and utilize its resources.

In this paper we will discuss the dependency of smart city on the infrastructure. The IoT network security is very important for the functionality of smart city. Any violation to the IoT devices will lead to spread the damage to other devices due to the sharing of devices.

With the big evolution of internet technologies and Wireless Sensor Network (WSN), a new communication technique is spreading; "Internet of Things" that represents a number of deployed objects or things that have communication between each other through network "machine to machine communication" or human to machine and that are exchanging data (Dieter et al. (2013) and (Al-Hamami. 2017)). Internet of Things (IOT) constitute of three main paradigms: object-oriented (sensors), internet-oriented

Wasan A. Al-Hamami, Mazin S. Al-Hakeem, Alaa H. Al-Hamami, 2023. Developing Smart City security through Upgrade Internet of Things Layers security. *Journal port Science Research*, 6(special), pp.39-44. https://doi.org/10.36371/port.2023.special.6

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 6 , special issue 2023

(middleware), and the exchanged knowledge (Al-Hakim. 2016 and Al-Hakim 2015).

IoT security involves safeguarding Internet-connected devices and the networks to which they are connected against threats and breaches, as well as finding, tracking, and fixing vulnerabilities from a variety of devices that may provide security hazards to your company.

One of the most sensitive issues faces this field is the security and privacy topics, where data can be stolen wirelessly and many other risks that will be discussed in this paper. Many researches have been conducted to eliminate these problems. The structure of this paper is as follows: part 2introduces the main IoT layers, part 3 represents the security goals, part 4discusses security challenges, part5explains security methods, part 6 represents security threats and part 7introduces the conclusion and future work.

2. ARCHITECTURE LAYERS OF IoT.

The majority of the workforce's issues can be solved by the internet of things in intriguing ways. The methodology used to arrive at a solution is based on how the information technology components were merged with communications systems, best hardware, and software convergence. In short, the software defined hardware system aids in the transformation of raw data into data input, from which advanced computing tools coupled with IoT systems perform data storing, retrieval, and analysis. IoT device use may be discouraged by rising security concerns such as software flaws and hacks among many consumers.

These IoT security issues are particularly important for businesses operating in the healthcare, finance, manufacturing, logistics, retail, and other sectors that have already begun implementing IoT devices.

The IoT architecture (A: three levels) (B: five layers). Observation, transit, processing, application, and business layers make up the five levels. The perception and layer and application layer play the same role as in a three-layer design. Sensing Layer – Sensors, actuators, devices are present in this Sensing layer. The other three layers are Network layer, Data processing layer and Application layer. The security in the IoT is the justification for adding a fourth layer. In a three-layer architecture, data is routed straight to the network layer. Sending data straight to the network layer increases the likelihood of encountering attacks. A new layer is suggested because the three-layer architecture has weaknesses. Information gathered from a perception layer and delivered to a support layer in a four-layer design.

The general architecture of an IoT system is divided with four layers as we suggested in this paper. The main layers of IoT shown as in Figure 1.

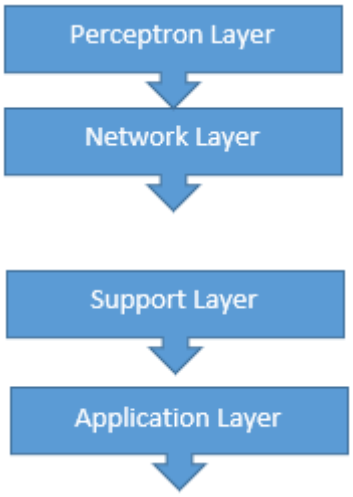


Figure 1: *IoT Layers.*

(a) *Perceptron Layer:* this layer has data sensor network in its different types, like Radio Frequency Identification (RFID) tags and barcodes, where these sensors identify different objects and collect data from the surrounding area and from other sensors. The sensing capabilities, information gathering, and information gathering about the environment where smart items are present are the features of this layer.

(b) *Network Layer*: This layer is made up of Wireless Sensor Networks (WSN), which use any helpful communication network to send data gathered from the preceding layer to a processing. The layer's ability to facilitate information processing and transfer with internet access for numerous devices is one of its features. Only when IoT systems are developed with security in mind can they be made secure, controllable, and private to smart users.

(c) *Support Layer:* Information-processing systems are in this layer where they perform suitable and automated actions depending on the obtained results of the gathered data from the perceptron layer, where these systems give different kind of services depending on its place and the required service from it, like remotely monitoring, managing and controlling devices.

The support layer is in charge of two tasks. It verifies that data is sent by legitimate users and is secure. There are numerous techniques to validate users and data. The authentication method is the most popular. It is carried out utilizing pre-shared passwords, keys, and secrets. Transmission of information to the network layer is the support layer's second duty. Information can be transferred wirelessly or over wires from the support layer to the network layer using this channel. This layer may be subject to a number of threats, including DoS attacks, malicious insider assaults, illegal access, etc.

(d) *Application Layer:* this layer includes the applications of IoT that makes cities smart, like Smart Parking,

Wasan A. Al-Hamami, Mazin S. Al-Hakeem, Alaa H. Al-Hamami, 2023. Developing Smart City security through Upgrade Internet of Things Layers security. *Journal port Science Research*, 6(special), pp.39-44. https://doi.org/10.36371/port.2023.special.6

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 6 , special issue 2023

Smart Phone Detection and Smart Lighting. The Its main feature of this layer is to deliver the specific service based on the application type to the user.

3. SECURITY GOALS OF IoT

There are three main IoT security goals that should be satisfied; Confidentiality, Integrity and Availability (CIA) [5, 6]. As shown in Figure 2.

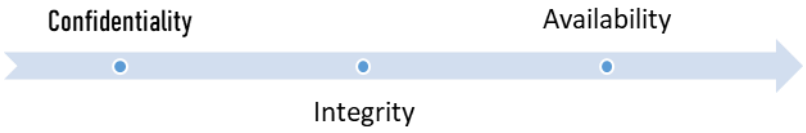


***Figure 2**: The IoT Security Goals*

(a) *Data Confidentiality***:** this goal guarantees the protection and keeps the privacy of the sensitive information of the users from the external intervention. This goal can be met by detecting and preventing the unauthorized access and allowing the authorized ones only. There are different mechanisms that achieve the goal of confidentiality, like data encryption and biometric verification. In the IoT point of view, sensor nodes and tags should not transmit their data to an unauthorized party (Al-Hamami. 2017).

(b) *Data Integrity:* this goal is to ensure that transmitted and received data, is protected from modification by any unauthorized party or other circumstances (damage of server). This data must deliver as it has transmitted. Many error detector mechanisms are applied to reach this goal, like the Cyclic Redundancy Check (CRC) and the Checksum.

(c) *Data Availability:* this goal of IoT guarantees that data is available for users; whenever the users want to access their data they can do so, despite of the situations even if it was normal or any problem has happened. Therefore, it is necessary to provide a powerful avoidance technique like firewall to prevent any attack to the services such as Denial of Service (DoS) attack that denies the data availability to the users. This goal also prevents the bottleneck issue that prevents the flow of information.

4. SECURITY CHALLENGES

a. Data transmitted in IoT are often personal, commercial, and industrial. These application data must be kept private and safe from all types of theft and tampering. The main difficulty with IoT is security. Among the several security challenges, the most significant and difficult are: a. Data privacy and security: Data must be protected against theft and kept secret from hackers while being transmitted without interruption.

b. Insurance issues: Insurance firms can install IoT devices on any application-oriented device.

c. Technical issue: Because IoT devices are being used excessively, more traffic is being created by them.

d. There is a lack of a universal standard for IoT devices. Authorized and unauthorized devices connected to the IoT system present the biggest challenge.

e. IoT systems primarily concentrate on various security difficulties in order to create adequate guidelines for network security and various security frameworks.

An IoT device's ability to connect to the internet and communicate with its surroundings by gathering and exchanging data is one of its key properties. Devices frequently only have a few specialized functions and a small amount of computational power (Atazori & Iera. (2010)). There are infinite ways IoT can be used and applied to various surroundings because devices come in such a wide variety. Each one of the mentioned layers has its own challenges, as described in the following:

4.1 Perceptron Layer Challenges: In This Layer We Have The Following Challenges:

1) Unauthorized access to the tags: tags in RFID systems can be accessed due to the lack of authorization methods, and so the attacker can alter or delete the data not just read it.
2) Tag cloning: the tags are visible and the attacker can access the data and change it by any hacking mechanism, so he/she can make a copy of the original tag without giving a chance to the reader to perceive between them.
3) Eavesdropping: since the communication between the tag and the reader is wireless, this allows the sniffing process possible from the attackers, and so they can take the sensitive information like the passwords.
4) Spoofing: the attacker can broadcast fake and false data to the RFID systems appears that it was sent from the original source so he can gain access (Gubbi et al (2012)).

4.2 Network Layer Challenges.

1) One such attack is the Sybil Attack, which manipulates nodes to offer many identities for a single node.
2) Sinkhole Attack: This kind of attack makes use of the compromised node (the node that the attacker has gained access to it) to make it attractive to other neighbor nodes to let them transfer the flow of data from them to the

Wasan A. Al-Hamami, Mazin S. Al-Hakeem, Alaa H. Al-Hamami, 2023. Developing Smart City security through Upgrade Internet of Things Layers security. *Journal port Science Research*, 6(special), pp.39-44. https://doi.org/10.36371/port.2023.special.6

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 6 , special issue 2023

compromised node, this leads to packet dropping and can lead to DoS attack.

3) Sleep Impairment Assault: Because the batteries in the WSN's sensors are limited, they follow a sleep schedule. In this form of attack, the attacker tries to disrupt the WSN's sleep schedule. to make the nodes a wake, to end their lifetime through consuming more energy and then to shut down.

4) Denial of Service (DoS) Attack: In this form of attack, the attacker overwhelms the targeted system with traffic, causing system exhaustion and preventing users from accessing the network.

5) Injection of harmful code: This form of attack, in which the attacker inserts malicious code into the system, is extremely risky, this can lead to a full shutdown of the network, or he/she can have a complete access and control to the network.

4.3. Support Layer Challenges.

a) Unauthorized Access: since this layer provides services, so if this process happens then it will forbid the access to the IoT services and may delete the data contained in it also, so the attacker can cause a complete damage of the system.

b) DoS Attack: it's same as discussed before where it leads to shut down the system and so the unavailability of the data.

c) Malicious Insider: In this case, the attack originates within, with an insider party manipulating the data for their own gain or the gain of a third party. An authorized user carries out the action to access another user's information. It is a very unique and sophisticated attack, necessitating various defenses to neutralize the danger.

4.4. Application Layer Challenges:

1) Malicious Code Injection: here the attacker uses hacking mechanism on the end-user system and steal some data from it through the injection of any kind of malicious code.

2) Spear-Phishing Assault: This is a spoof email attack. where the targeted user opens an email from the adversary and by that the attacker can gain access and take more sensitive information.

3) Sniffing Attack: here the attacker uses a sniffing application on the victims' system, which leads to information gain from the network.

5. SECURITY METHODS IN LAYERS.

The security in the IoT layers concluded in Figure 3.

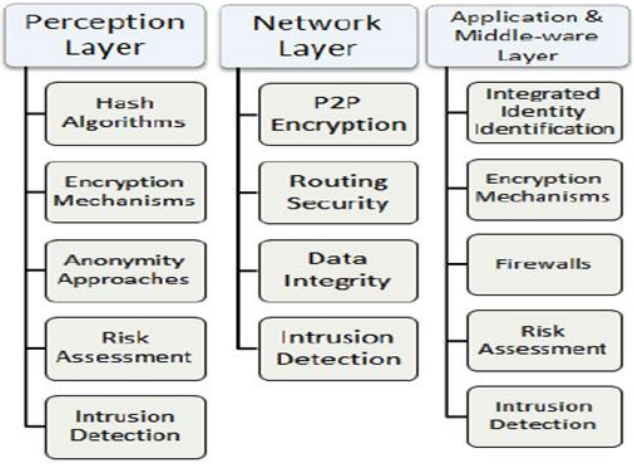


***Figure 3**. IoT Layers Security*

Figure 3 describes the security methods that are used in each layer, that are illustrated in the following part:

(A) *Perception Layer:* this layer provides four security services for the hardware, that are described as follows:

1) Authentication: This is carried by via cryptographic hash methods that employ digital signatures on the terminals, which must be able to withstand all known assaults, including side-channel and collision attacks.

2) Data Privacy: we can guarantee the Through symmetric and asymmetric encryption, data privacy is ensured. techniques, so the unauthorized party will be prevented from accessing the sensor data in the collecting or forwarding processes.

3) Sensitive information privacy: The sensitive data like the identity, location and some others need to be hidden for protection purpose, so the anonymity approach is used, like K-anonymity property.

4) Risk Assessment: it's so essential for the IoT security, where the threats are discovered on the system. Security breaches are prevented and the best security strategy is determined in this strategy like Dynamical Risk Assessment method for IoT (Farooq et al. (2015)).

Despite of all these security strategies an intrusion may happen, and if that intrusion was in order to prevent unwanted access to the RFID tag data when this is detected, a kill-command is issued from the RFID reader to the RFID tag (Abdul Rahman et al. (2014)).

(B) Network Layer: Because wireless communications are open, this layer is vulnerable to **attacks.** network channels, this layer is divided into the following security measures, which are illustrated as the following (Zhang et al. (2012):

1) Authentication: For a purpose a suitable authentication procedure and Point-to-point encryption has been implemented, preventing

Wasan A. Al-Hamami, Mazin S. Al-Hakeem, Alaa H. Al-Hamami, 2023. Developing Smart City security through Upgrade Internet of Things Layers security. *Journal port Science Research*, 6(special), pp.39-44. https://doi.org/10.36371/port.2023.special.6

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 6 , special issue 2023

unauthorized access to nodes that disseminate bogus information. The DoS attack is the most common one in this layer.

2) Routing Security: this process is done to guarantee the confidentiality of the data exchange between the processing systems and the sensor nodes. Multiple paths are provided to ensure the security, by detecting the secure path and perform the data exchange through it. There are many researches have been done for the routing techniques purpose, like Source Routing and Hop-by-Hop routing.
3) Data Privacy: there are safety control techniques that are applied on the system to ensure the protection from any kind of intrusion, and we have ensured that the received data was not modified (received as it was sent) through data integrity techniques.
4) Data transport assaults: In core networks, many attacks on the data security and integrity take place during data transit.
5) Spoofed Routing Knowledge: To disrupt network traffic, attackers' spoof, alter, or reply IP addresses. This leads to router loops, bogus error messages, reduced routes, etc.

(C) *Support and Application Layer:* the merge of these two layers was done to constitute an integrated security mechanism, as illustrated in the following (Kargianni et al. (2007)):

a) Authentication: prevent any illegal access, here users choose to share their information with the services. The main used technologies in this layer are the cloud computing and the virtualization.
b) Intrusion Detection: A continuous monitoring and a log of disturber's activities are done over here, to detect any anomaly activity and generate an alarm if so.
c) Risk Assessment: This gives a reasonable reason for using an effective security methodology and expands the currently used security structure.
d) Data Security: This is done through many encryption techniques to prevent data stolen from any intruder.

6. SECURITY THREATS

There is a number of well-known and widespread security threats that faces the Internet of Things, some of them are mentioned as the following.

a) Insufficient authorization: this appears when the attackers gain access and they without any authorization.
b) Insecure network services: this is due to buffer overflow attack or DoS attack.
c) Absence of transparent encryption: the data is viewed in its plaintext state in its transmission over the network.
d) Insufficient security configurability: this occurs when the device users can't change the security controls.
e) Lacking of physical security: there is a lack of protection of the sensor where they are susceptible for stolen.

7. CONCLUSION AND FUTURE WORK.

In recent years IoT has become the area of interest and will be for the next coming years. In the context of the rapid evolution many problems have been risen and one of the most important of them is the security and privacy issues. We have been discussed data confidentiality, integrity and availability, in addition to the security challenges that faces each layer, the security methods and the most popular threats in IoT.

Smart City provides human with quality of life when it offers the perfect services for its residents. This perfectionism can be accomplished by providing secure, integral, and private data to the Thinks in the Internet of Things. As the security and privacy of Internet of Things network are strong, the smart city will work perfectly without problem. As a future works a secure framework of IoT that preserves the security and privacy principles could be constructed, and Internet of Things protection Methods could be recommended.

REFERENCES

[1] Abdul Fuad Abdul Rahman, Maslina Daud, Madihah Zulfa Mohamad, (2013). Securing Sensor to Cloud Ecosystem using Internet of Things (IoT) Security Framework, My Cyber Security Clinic (MyCSC) Cyber Security Malaysia.

[2] Al-Hakim M S & Al-Hamami A H.(2016). Implementation of common secure framework for IoT Based Arduino platform, International Journal of Computer Trends and Technology (IJCTT), Volume 32, Number 1.

[3] Al-Hakim M S & Al-Hamami A H. (2015). Proposed Flip Teaching Framework Based on Multi-Tier Architecture, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 6.

Wasan A. Al-Hamami, Mazin S. Al-Hakeem, Alaa H. Al-Hamami, 2023. Developing Smart City security through Upgrade Internet of Things Layers security. *Journal port Science Research*, 6(special), pp.39-44. https://doi.org/10.36371/port.2023.special.6

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 6 , special issue 2023

[4] Al-Hamami A H & Al-Hakim M. (2017). Everything about Internet of Things and Smart Cities Applications, Dar Al Raya for Publication and Distribution, Amman, Jordan.

[5] Farooq. M. U, Muhammad Waseem, Anjum Khairi, Sadia Mazhar February (2015). A Critical Analysis on the Security Concerns of Internet of things (IoT), International Journal of Computer Applications (0975 8887).

[6] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, Marimuthu Palaniswami. (2013). Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions, Elsevier.

[7] Kargianni.S. T, Eydt. B, Barber. G, Bunn. L, Phillips. T. (2007).Guidelines for Securing Radio Frequency Identification (RFID) Systems, in Recommendations of National Institute of Standards and Technology.

[8] Liu. C, Zhang. Y, Zeng. J, Peng. L, Chen. R. (2012). Research on Dynamical Security Risk Assessment for the Internet of Things inspired by immunology, in Eighth International Conference on Natural Computation (ICNC).

[9] Luigi Atzori, Antonio Iera. (2010). Giacomo Morabito, The Internet of Things: A survey. 2787–2805, ELSEVIER.

[10] Sean Dieter Tebje Kelly, Nagender Kumar Suryadevara, and Subhas Chandra Mukhopadhyay. (2013). Towards the Implementation of IoT for Environmental Condition Monitoring in Homes, IEEE SENSORS JOURNAL.

Wasan A. Al-Hamami, Mazin S. Al-Hakeem, Alaa H. Al-Hamami, 2023. Developing Smart City security through Upgrade Internet of Things Layers security. *Journal port Science Research*, 6(special), pp.39-44. https://doi.org/10.36371/port.2023.special.6