International Journal of Latest Engineering and Management Research (IJLEMR)
ISSN: 2455-4847
www.ijlemr.com || Volume 06 - Issue 09 || September 2021 || PP. 27-37

Cyber security of internet of things platform, Smart home as example

Ahood Hameed S. ALThobiti
Samah Mohammed S. ALHusayni
#student in cyber security master
Taif Universty, Taif21944,Saudi Arabia

Abstract: Technology accelerates development day after day to provide many services and link them together, which makes life more luxurious and easy than before. Internet of things is one of these advanced technologies, which are increasing in size and uses in our reality, and their applications vary from smart cities, smart homes, industrial and smart health systems, and many more prominent. Topics that have taken place in a researches and investigation are how to securing the Internet of things, especially as it was initially manufactured without taking into account security essentially when designing.

This paper focused on security in IoT systems, It present the IoT architecture, the most attacks in the IoT and countermeasures , studying a smart home security issues and simulate smart home environment with cisco packet tracker and produce security recommendations to enhance security in IoT.

Key word: challenges; internet of things; IoT attacks; machine learning; security solution

1- Introduction

Security of Internet of Things gadgets has become a consuming inquiry in the twenty-first century. In one side, IoT brings everything close and associates the entire world, other hand, it opens different windows to be misled by various sorts of assaults. In spite of the fact that the term IoT is short in its setting shrewd, it contains the whole world with its keen advancements and administrations that can be envisioned. The word IoT was first utilized by Kevin Ashton in quite a while research introduction in 1999[1]. From that point, IoT is being utilized to build up a connection among human and virtual world utilizing different savvy gadgets with their administrations through various correspondence conventions. What was a fantasy 25 years prior is currently a reality with the assistance of IoT. In single word, the present progressed world is wrapped by savvy innovation and IoT is its core. Presently, individuals can't think a solitary second without anyone else without utilizing IoT gadgets and their administrations. A study shows that almost 50 billion things will be associated with web by 2020 and it will increment exponentially as time passes by[2]. It is likewise assessed that IoT will catch around 3.9−11.1 trillion USD affordable market by 2025 [3]. Thusly, research on IoT and its turn of events and security has gotten enormous consideration in the course of the most recent a very long time in the field of electrical and PC since. In this paper we present the IoT architecture Then the most attacks in the IoT and countermeasures then study a smart home as example of IoT app to clarify requirements, security objectives, most attack which faces smart home ,cryptography suitable to smart home system , simulate smart home environment and produce security recommendations to enhance security in IoT.

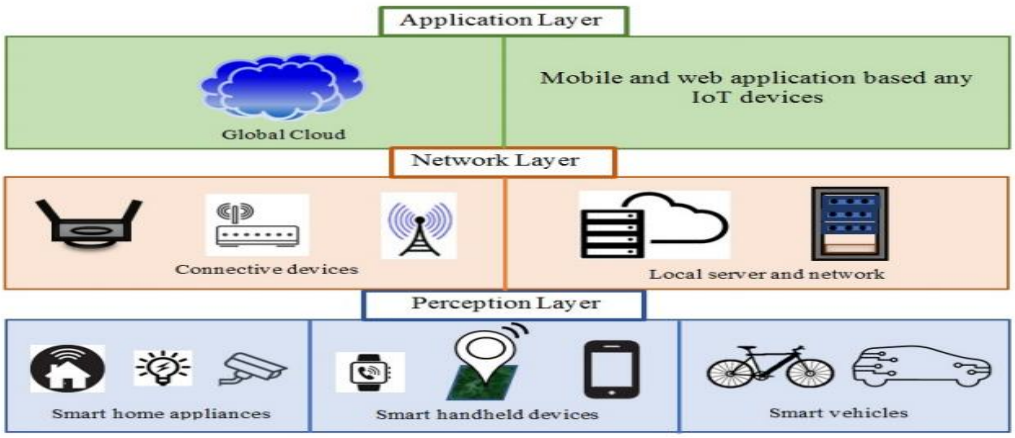

Figure 1:Internet of things layers[4]{Tahsien, 2020 #4}

2- IoT Layers architecture

The design of IoT, which is a passage of different equipment applications, is created so as to build up a connection and to extend IoT administrations at each doorstep. Distinctive correspondence conventions, including Bluetooth, WiFi, RFID, thin and wideband recurrence, ZigBee, LPWAN, IEEE 802.15.4, are embraced in various layers of IoT engineering to communicate and get different data/information[4],[5]. Also, huge scope innovative organizations have their own IoT stages to serve their significant clients, for example, Google Cloud, Samsung Artik Cloud, Microsoft Azure suite, Amazon AWS IoT, and so forth. A standard engineering of IoT comprises of primarily three layers i.e., recognition/physical layer, network layer, and web/application layer as shown in Fig 1.

2.1. Application Layer

The application layer is the third layer in IoT frameworks which offers support to the clients through portable and online virtual products. In light of late patterns and utilizations of keen things, IoT has various applications in this mechanically progressed world. Living space/homes/building, transportation, wellbeing, instruction, farming, business/exchanges, energy dispersion framework, and so forth have gotten savvy by the beauty of IoT framework and it uncounted help.

2.2. Network Layer

The organization layer is more significant in IoT frameworks since it goes about as a transmission/diverting vehicle for data and information utilizing different association conventions, including GSM, LTA, WiFi, 3-5G, IPv6, IEEE 802.15.4, and so forth, which interface gadgets with brilliant administrations. In the organization layer, there are nearby mists and workers that store and cycle the data which functions as a center product between the organization and the following layer. Enormous information is another significant factor in the organization layer since it draws in the consideration of the present ever3 developing conservative market. The physical articles from the physical layer are creating an enormous measure of data/information ceaselessly which are being sent, handled, and put away by IoT frameworks. Since data/information are significant for brilliant administrations in the organization layer, ML and Deep Learning (DL) are widely utilized these days to investigation the put away data/information to use better examination methods and concentrate great uses from it for savvy gadgets.

2.3. Perception Layer

The primary layer of IoT design is the observation layer which comprises of the physical (PHY) and medium access control (MAC) layers. The PHY layer essentially manages equipment i.e., sensors and gadgets that are utilized to send and get data utilizing distinctive correspondence conventions e.g., RFID, Zigbee, Bluetooth. The MAC layer builds up a connection between physical gadgets and organizations to permit to for legitimate correspondence. Macintosh utilizes various conventions to connect with network layers, for example, LAN (IEEE 802.11ah), PAN (IEEE 802.15.4e, Z-Wave), cell organization (LTE-M, EC-GSM). The majority of the gadgets in IoT layers are attachment and play types from where a gigantic bit of enormous information are created.

3- Attacks in IoT communication

The term Internet of Things is spread widely without absolute explanation due to the multiplicity of technologies that depend on it, such as machine-to-machine communications, wireless sensor networks and radio frequency identification[6].Today, its applications have become large and promising as areas of intelligence in cities, cars, smart homes, and the like, making them more vulnerable to the exploiting attack .There is a challenge in providing reliable and safe Internet of things services due to its dependence on the Internet and their association with physical parts directly increases these[7].

In the course of the most recent couple of years, the IoT framework has been confronting various assaults which make the makers. Clients cognizant with respect to creating and utilizing IoT gadgets all the more cautiously. This segment depicts diverse sort of assaults, their belongings, and assault surfaces in IoT.

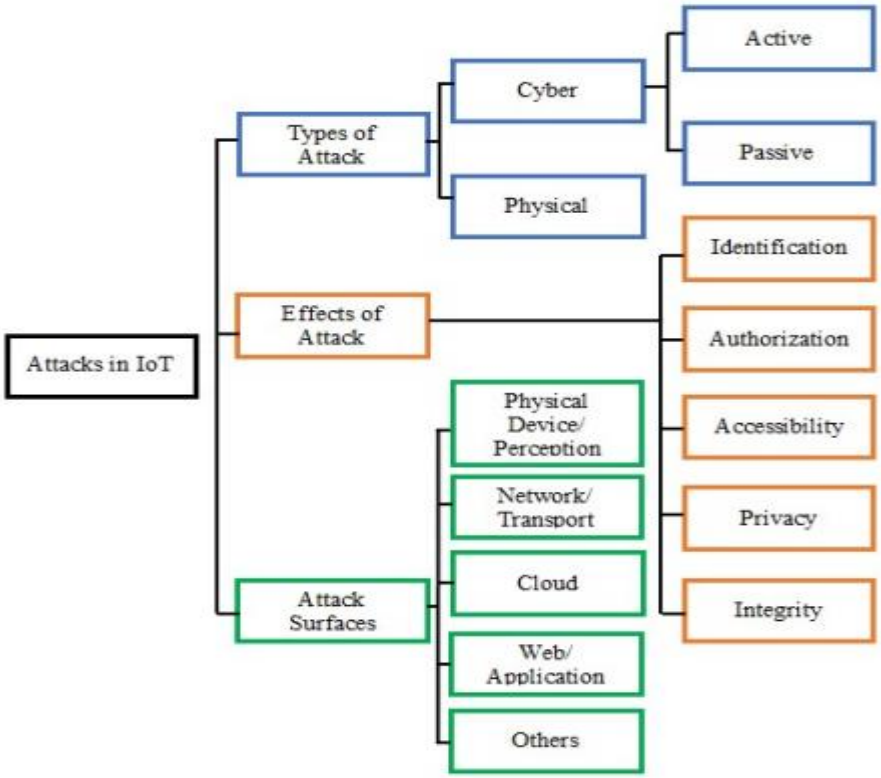

Figure 2: An outline of an itemized rundown of IoT security assaults that incorporates various kinds of assault, assault surfaces, and assault impact[4].{Tahsien, 2020 #4}

The following are some types of attacks

3.1 Attacks on side channels

This attack has an impact on the protection of encryption methods and it is hard to identify the attack at the level of the end nodes, making it difficult to protect and we can restrict the attack by reducing leakage and bringing noise[6].

3.2 Collision attacks

The attacker creates many collisions and by resending many of affected packets, the target's battery is effortlessly exhaustion[8].

3.3 Fragmentation attacks:

There are many protocols used in the Internet of Things due to the multiplicity of networks and the purposes of their use, which leaves room for penetration. For example, 6loWPAN lacks security technologies such as authentication, which makes it easy for the hacker to add malicious packages between other fragments of the packet[9].

3.4 Routing attacks

The modification of the routing data, so named modifying attack, is the simplest routing method for attacks used I spoofing , dropping packets , Sybil[10] ,Hello flood[9]and Gray Hole[11]

3.5 Eavesdropping

Eavesdropping is spying on the access channel to gain access to communication packets, and if it is not encrypted, it will be easy for him to know the parties involved and passwords, and he may access larger data that is easy for him to access, such as a shared key[6]**.**

3.6 inject malicious packets:

Malicious packet insertion attacks rely on capturing and modifying the packets by inserting, copying, or modifying the packets[8] to make them look legitimate and then sending them over a connection link to be exchange over the network.

3.7 Unauthorized access

Each entity in the Internet of things interacts with other entities to communicate and share data, which is necessary[6]. The interaction is limited to the mutual objects of their data to restrict unauthorized access to IoT objects, which causes a danger that extends to other things**.**

3.8 Dos attack

It hinders the passage of packets and services become unavailable in multiple ways, including intermittent jamming that allows for packets to be exchanged intermittently, that is, partial interference in the network, and the other type, complete interference that prevents sending and receiving packets[6].For example, in case of an emergency an intruder may block a fire sensor system from notifying a fire department by jamming its communication link[12].

3.9 Assault Desynchronized

The attacker spoofs the serial number of the forged packets, hindering active communication between the real packets, i.e. causing an out of sync between them[6].

4- Countermeasure of IoT attack

There are some measures and measures taken to protect or mitigate against attacks in the Internet of things[13]. Each layer can be assigned what suits it and can be dealt with in general and on a large scale[13] as we will present in this paper.

4.1 Trade-Offs Features

Due to the restricted resources funded on IoT devices, trade-offs in features and system specifications should be taken on all related IoTlayers[14, 15].Throughout to better handle these feature trade-os when preserving the highest degree of protection, some frameworks can be adapted[13].

4.2 Security of physical layer

The use of technologies that mask data and sensitive information such as zero-based information[16] and anonymity helps provide physical layer security. Physical protection can often reduce risks in other layers at the same time[13]. The overlap design of the functionalities in IoT ensures that a more protection environment can results in more secure implementation and computing layers[13].

4.3 Risk valuation

With pre-existing architectures and especially the application layer, risk assessment can reduce the impact of vulnerabilities[14, 17]. Dynamic risk valuation approaches include confidentiality and help prevent security , in particular on the physical layer[18].

4.4 Security of network

use routing algorithms secures networks from adversary attacks by applying security measures to packets[19]. Anonymity is extended to sensor entities in the Internet of Things[14, 20]. We use protocols that provide more security, so with TCP we use SSL / TLS Helping to reduce the Eavesdropping and man-in-the-middle[21], with UDP we use DTLS[21] and instead of IPv4 to IPv6[22]**.**

4.5 Distribution of keys

As often as cryptography and encryption algorithm are essential to the protection of all transmission of data, key distribution reduces cyber-attack dangers and can operate within lightweight implementations[23].

4.6 Encryption and Cryptography

Data encryption is a fundamental pillar in preserving data from hacking or eavesdropping, and in providing security at all points in the Internet of things at the level of devices, networks and mobile data. Regardless of whether it is symmetric or asymmetric, generally due to hardware limitations, methods that uses less energy are recommended**.**

4.7 Digital signatures

Digital signatures, mostly epitomize in hybrid cryptographic technology models, are one particular cryptographic technique used in heterogeneous deployments to avoid hacking attacks and maintain the security and protection of data transmission. These method requires low process speeds than techniques like AES and quicker than RSA[24].

4.8 Protocols on Processing

Computing layer protocols, such as "Fragmentation Redundancy" scattering, reduce data breaches by separating and assigning data to fragments between clouds and direct transfer among devices. End-to - end data security mechanisms are ideally suited for transmissions that occur in this layer, as well as for maintaining data protection throughout its life cycle among computers[14]

4.9 Application Security

Security on the application layer will control activity by filtering and/or blacklisting input and output applications via access control lists[14, 25]. The valuation of protocols applied in the application layer can support to equilibrium risk with functionality. Service Level Agreement (SLA)m and Virtual Machine Monitor(VMM) are procedures used in the application layer along with IDS in order to realize accessibility and keep data through stoppage or malicious attacks[22].

4.10 Patching

Daily IoT-device upgrades to applications and operating systems can help alleviate endpoint weaknesses and reduced risk[13].

4.11 Detection of intrusion

Intrusion Detection Systems (IDS) protect environments by generating alerts whileobserving risks that are either aggressive, malicious or unknown within the application layer[14, 23, 25, 26].Intrusion and danger monitoring is used to fix bugs which are not detected by visible defense strategies or antivirus software; when anomalies are registered, logs can be tracked to malicious or suspicious behavior[13].

4.12 Antivirus / Firewalls

Web app detectors will help locate vulnerabilities, particularly when installed within firewalls to predict possible attacks. Firewalls, while implemented alongside ACLs, will prevent illegal entry and help with packets filters on the application layer[13].

4.13 Blockchain

Many studies show blockchain as a multiple layer approach to secure IoT networks. Blockchain platforms may be implemented whether in centralized or decentralized modeling techniques with their own vulnerabilities and strengths[13]. The former is best suited for the handling of massive data transmissions from heterogeneous devices, and another is best suited for accessibility and real-time operations[13].

4.14 Detection of Honeypot

Honeypot detector is yet another type of device and network infrastructure centered intrusion and/or risk mitigation. Rather than merely recording weaknesses or threats, honeypot detecting helps deter attackers by providing a different zone beyond the normal network reach, known as the "DMZ;" with this method, weaknesses may still be identified and logged without placing the remainder of the IoT network at greater danger[14, 27].

4.15. Standardization

The lack of uniform specifications for IoT devices has existed in a relatively heterodox area, that has causes in difficulty in the development of device protection measures[13].The most important to standardization is the network layer instead of the physical layer[13]. Standardized protocols create a unified secure, and simpler environment via devices communicates[22, 25].

4.16. Filtering Traffic

Scanning traffic signals among devices on a physical layer and filtering it , often without IDS or vulnerability scanning on software-based layers, is one way to protect IoT networks and avoid harmful signals or cross-communication[13].

4.17 Protection Node-to-Node

End-to - end encryption reduces dangers of all wireless technology between systems, regardless of the protocol implemented; however, separate suites should be used based on the protocols applied within the related layer[28]. likewise, point-to - point communication solutions, which can form the basis of IPsec VPNs or MPLS, have the same secure as end-to - end communication protocols, but with higher energy usage needs[22, 23].

4.18 Authentication

Strong authentication is essential for alleviating threat throughout all layers. The system verification and recognition must occur on the physical layer before the information is transferred or obtained[29].Authentication protocols prohibit unauthorized entry to sensor content in the network layer. A very popular form of attack on this layer is DoS hacks, which can help avoid authentication[14].

4.19 Trust Institutions

Machines would usually be capable of reaching third parties or, by definition, have these confidence stores integrated into their architecture. Trust stores help to protect standardized transaction records and avoid untrusted interactions and threats, however, based on their application, they must still be balanced against reverse engineering threats or the use of continuous remote authentication[28].

4.20 Active defense

In comparison to spyware or firewall applications, deep packet inspection has been suggested as a tool for detecting suspicious content or activity in actual time[13].Active defense can be considered the key section of the defense structure and can embed a variety of other method; Like recovery, verification, access management, and cryptography; but, this is dependent on either the machine's needs and capabilities[13].
Since active defense cannot repel all attacks, it must use other countermeasures with it[27].

4.21 Data protection depending on location

GPS hacking happens as an assault on the network layer. Methods like the GPS Positioning Technique[30] have been used to effectively minimize localized device attacks. Authentication , and also geo-spatial authentication, is used to tackle a very critical attacks[31].

5- Methodology

Our methodology is study a smart home as example of IoT app to clarify requirements, security objectives, most attack which faces smart home,cryptography suitable to smart home system , simulate smart home environment with cisco packet tracker network and produce security recommendations to enhance security in IoT.

5.1 Security in Smart Home

The utilizations of an IoT at shrewd home frameworks depend on the accommodation to access home apparatuses all over the place and whenever, not just restricted to whether clients are inside or outside of their home. The fundamental issue that rises in the shrewd home framework is network security where all gadgets associated with the web are very powerless against programmer assaults [32] .Programmers can break (misguidedly sneaks around) into the worker and recover significant data (for example personal residence, data about home gadgets, and harm the keen home framework). A decent security viewpoint and sufficient solace of an IoT based savvy home are positively significant and very required [33] ,it is real to be executed so as to permit a completely "protection control" to the clients [34].In the other hand, a productive system for making sure about the home apparatuses associated with the web is additionally concerned[35, 36].

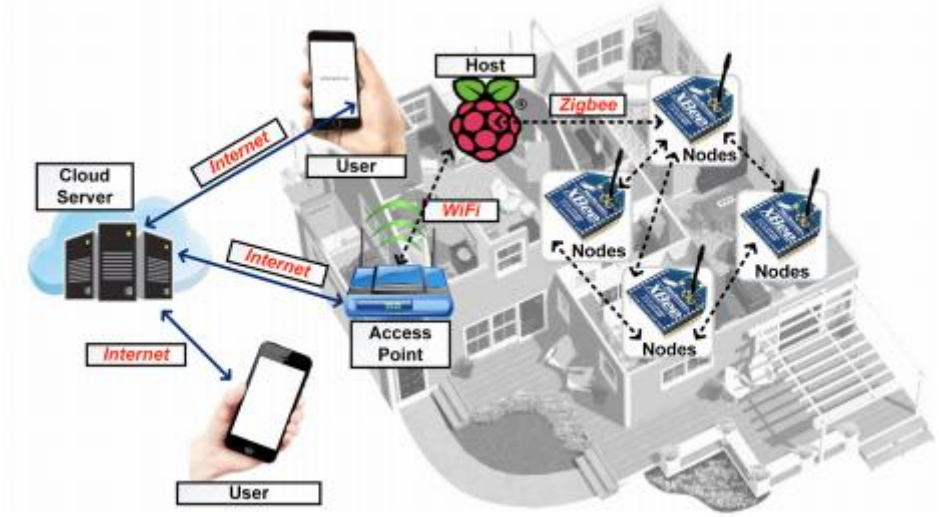

Figure 3. Block diagram of developed smart home system[36]

5.2 SMART HOME ENVIRONMENT SECURITY ISSUES

5.2.1. Requirement for Security for the Smart Home Environment

IOT security must be incorporated into each hub of the framework in any case a shaky part in the organization could be a state of assault and can make the entirety framework defenseless. That is the reason security must prevail in each part of the plan of IOT application that will require a significant level of security. Clearly with no defensive instrument, the organization could endure from assaults or breakdowns that upset the administrations gave by the organization [37].Care ought to be practiced in recognizing potential dangers and assaults, for example, infusion and additionally alteration of information bundles that can prompt undesirable circumstances and cause interruption in the organization and applying the standard strategies for security against them[38].

5.2.2. Security Goals

The security targets of electronic data are resolved dependent on the sorts of dangers and weaknesses that can be exacted upon it. While weakness manages the occasion to cause harams a result of an intelligent plan or usage defect, a danger emerges from an aggressor attempting to discover and abuse the weakness so as to dispense harm. When managing security in IOT, coming up next are some fundamental security prerequisites that are frequently the measures to analyze the exhibition of different made sure about frameworks:

5.2.2.1 Confidentiality

The property of information to be available only to an authorized user group . It refers to preventing disclosure of information to unauthorized persons, parties or systems[38] .

5.2.2.2 Integrity

The property of information to be protected against unauthorized modification more specifically in the automation system, this applies to information such as sensor values, or control commands[38] .

5.2.2.3 Availability

The property of information to be available in unreasonable time frame . It refers to ensuring that unauthorized persons or systems cannot deny access system resources to authorized users[38] .

5.2.2.4 Authenticity

The property to be able to identify the author of an information .authentication distinguishes between legitimate and illegitimate users in a system [38] .

5.2.2.5 Freshness

It could mean information newness and key newness. It is worried about whether the information delivered or estimated in the framework is later and guarantees no foe produced old messages.

5.3 attributes of attacks and countermeasures

The diversity of communications between devices and sensors makes these targets vulnerable to attacks, and the smart home can identify security targets based on the function of the device, and we will show the most prominent attacks faced by such communications[38].

5.3.1 Spying attack

Spying is an outer threat where an opponent will actively wake up in contact with the web and snatch the content to breach the anonymity of messages by web interception and sniffers or listened to packet forwarding[38].

Protection with verification and integrity measures can avoid some deliberate spying and defining jamming and redirecting of packets[38].

5.3.2 DDOS attack

Attacks are carried out by sending a steady stream of data packets with an aim to causing conflicts[38]. This conflicts cause the sensors to relay signals forever and to make them inaccessible by wasting battery life[38]. As an outcome, the sensors use important computing energy, such as capacity and processor power and setup resource disturbance[38].

Protection with a probability metrics against counter-collision is done randomly back-offs that reduce the collision rate and the MAC constrain rate and use smaller frame sizes[38].

5.3.3 Compromise Node

This is achieved anytime a legal node inside the system is identified and hacked[38]. Attacker may utilize a computer that is more effective in terms of computer and wireless energy to connect with sensors and inject malware coding without going to their places or actually contacting them, theft information from encrypted data, reporting inaccurate and deceptive data to the web, review other legal nodes as malicious node, and conducting various routing activities[38].

Defend using code validation schemes that use an effective application user authentication to prove the ram of the sensor node by computing the hash code of chosen randomly memory areas[38].

5.3.4 Sinkhole and Wormhole

Sinkhole is a piece of malware in which a compromised actor brings packets of data to it by disseminating untrue routing information to its friends in order to selectively forward nodes that in turn, rearranges the forwarding system's behavior by suppressing or modifying traffic as it would like[38]. Wormhole Damage, is an intruder collects traffic at one node in the system, transfers them to another node in the system, and then replays these packets on the system at this node on, causing chaos in forwarding, aggregation, and other critical choices made by the nodes[38].

Defend by making each component use a special symmetric encryption exchanged with the center so building effective forwarding algorithm, such as multi-path forwarding, will assist mitigate the impact of these activities[38].

5.3.5 Physical Attack

The capability of the intruder to achieve actual exposure to the devices. This real access allows up a variety of threats, involving deleting or capturing sensors, deleting packets from their current forms, injecting malware, and extracting confidential info like encryption algorithms[38].

securing by Tamper Security Evidence Hardware, but it's still costly and might not be much more successful towards an intruder[38].

5.4 cryptographic techniques

Cryptography is the standard encryption process employed in the secure application of packets exchange to secure data transfer protection measures to be implemented into each node of the web[38]. There are two main kinds of encryption algorithms, symmetric and asymmetric[38]. In WSNs, symmetric encryption has been the perfect solution because nodes hardly tend to devote their minimal resources to the implementation of complicated and resource-oriented public - key encryption[38]. AES It is grown rapidly in sensor nodes since it is much quicker, uses fewer energy and is ideal for various sizes of the processor[38]. AES stands with 128-bit frames and has a key length of 128, 192, or 256 bits. Nowadays a key length of 128 bit is made successful sufficiently[38].

5.5 Simulation of smart home

The smart home is one of the applications of the Internet of things, and it is intended to manage and control smart home devices remotely, such as opening the lights, turning on the air conditioning, monitoring the water level, opening and closing doors and windows and more, and all of these operations must be carried out under a high security level.

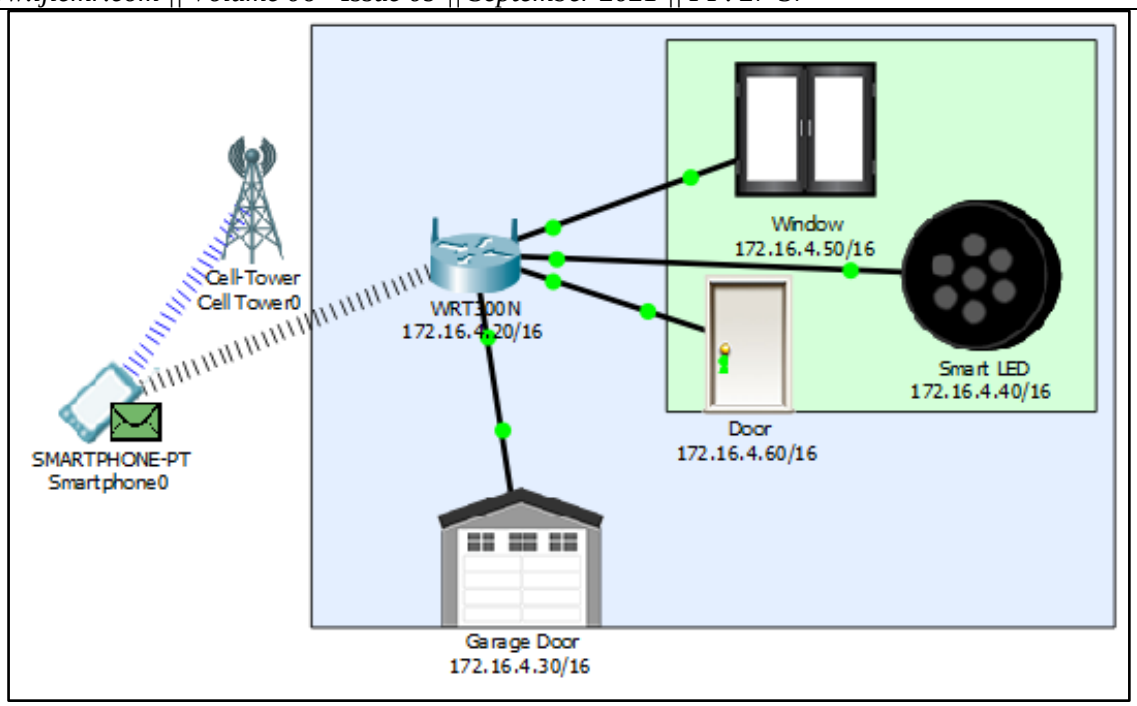

Figure4.Simple simulation to smart home with Cisco Packet Tracer network simulators.

This picture shows the simplest components of a smart home which is a smart garage door, smart room door,smart window and lighting all connected to a wireless home router. As well as a smart computer that can connect to the wireless router and control devices. It can also control smart devices remotely through its connection to the Internet via a cellular network when it is outside the coverage area of the wireless.

The aim of this simulation is a graphic representation of the diversity of devices from constrained devices like sensors , computer ,smart phone, server to multi kind of networks like Wi-Fi , cellular networks and so that used in the Internet of Things, which in turn affects the level of security in the Internet of Things. Just as this diversity has a role in enhancing flexibility at the system level in designing things[39], this diversity is a challenge in the field of security for the Internet of things. So these are some recommendations that enhance the level of security in the Internet of Things. We concluded it by linking above simulation with concerns and factors affecting the security of the Internet of Things mentioned in[40].

1- Updating operating systems to raise security for devices periodically, which reduces the opportunities for attackers to exploit to carry out malicious attacks
2- Changing the default passwords of the devices to block one of the most prominent methods of attackers to penetrate
3- Tracking any attempts to access the devices or the network, and the application that connects the user with smart devices helps in that.
4- Since the smart home depends on remote access operations through wireless networks such as Wi-Fi, Bluetooth, ZigBee, and Z-Wave, these networks must be secured, for example by using stolen words on Wi-Fi and supporting them with appropriate encryption algorithms as well as keeping them in safe places that intruders cannot reach
5- Download reliable and high-security programs to manage and provide smart home services, as people may be deceived by the advantages offered from one application to another, and therefore it must balance between security and available functions
6- Using strong authentication to make sure of the validity of the user, such as a fingerprint, for example, because successful authentication reduces the chances of impersonation.
7- Keeping smart devices and sensors in safe places or saving their chips in a tamper-resistant way, so that if the device is reached, it cannot come out with information about the encryption algorithm used or data that helps penetration.
8- Install anti-virus programs , intrusion detection and update these supported security programs to more secure environment.

Conclusion:

In this research, the most important attacks facing the Internet of Things and defense methods were addressed, then the smart home was dealt with as one of the Internet of Things applications to clarify the system in a simple way and identify the most prominent challenges facing the Internet of things, which is the diversity of devices from resource-restricted devices, computers, smart phones, various networks and thus multiple protocols, which makes security In a critical situation, some advice was provided that enhances safety in the Internet of things. We recommend that devices be designed according to security with the function for which they are made, as well as choosing protocols, encryption and security methods suitable for the varying needs of the Internet of things**.**

References:

[1]. K. Ashton, "That 'internet of things' thing," *RFID journal*, vol. 22, no. 7, pp. 97-114, 2009.
[2]. M. A. da Cruz, J. J. Rodrigues, A. K. Sangaiah, J. Al-Muhtadi, and V. Korotaev, "Performance evaluation of IoT middleware," *Journal of Network and Computer Applications*, vol. 109, pp. 53-65, 2018.
[3]. J. Manyika *et al.*, "Unlocking the Potential of the Internet of Things," *McKinsey Global Institute*, 2015.
[4]. S. M. Tahsien, H. Karimipour, and P. Spachos, "Machine learning based solutions for security of Internet of Things (IoT): A survey," *Journal of Network and Computer Applications,* vol. 161, p. 102630, 2020.
[5]. M. Saadeh, A. Sleit, K. E. Sabri, and W. Almobaideen, "Hierarchical architecture and protocol for mobile object authentication in the context of IoT smart cities," *Journal of Network and Computer Applications*, vol. 121, pp. 1-19, 2018.
[6]. Z. Dawy, W. Saad, A. Ghosh, J. G. Andrews, and E. Yaacoub, "Toward massive machine type cellular communications," *IEEE Wireless Communications*, vol. 24, no. 1, pp. 120-128, 2016.
[7]. H. A. Abdul-Ghani and D. Konstantas, "A comprehensive study of security and privacy guidelines, threats, and countermeasures: An IoT perspective," *Journal of Sensor and Actuator Networks*, vol. 8, no. 2, p. 22, 2019.
[8]. D. M. Mendez, I. PapapanagIoTou, and B. Yang, "Internet of things: Survey on security and privacy," *arXiv preprint arXiv:1707.01879*, 2017.
[9]. J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary, "Wireless sensor network security: A survey," *Security in distributed, grid, mobile, and pervasive computing*, vol. 1, no. 367, p. 6, 2007.
[10]. I. Tomić and J. A. McCann, "A survey of potential security issues in existing wireless sensor network protocols," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1910-1923, 2017.
[11]. A. Rajan, J. Jithish, and S. Sankaran, "Sybil attack in IOT: Modelling and defenses," in *2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, 2017: IEEE, pp. 2323-2327.
[12]. P. Rani, S. Verma, and G. N. Nguyen, "Mitigation of Black Hole and Gray Hole Attack Using Swarm Inspired Algorithm With Artificial Neural Network," *IEEE Access*, vol. 8, pp. 121755-121764, 2020.
[13]. A. Mosenia and N. K. Jha, "A comprehensive study of security of internet-of-things," *IEEE Transactions on Emerging Topics in Computing*, vol. 5, no. 4, pp. 586-602, 2016.
[14]. M. A. Obaidat, S. Obeidat, J. Holst, A. Al Hayajneh, and J. Brown, "A Comprehensive and Systematic Survey on the Internet of Things: Security and Privacy Challenges, Security Frameworks, Enabling Technologies, Threats, Vulnerabilities and Countermeasures," *Computers*, vol. 9, no. 2, p. 44, 2020.
[15]. A. W. Ahmed, M. M. Ahmed, O. A. Khan, and M. A. Shah, "A comprehensive analysis on the security threats and their countermeasures of IoT," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 7, pp. 489-501, 2017.
[16]. G. Rajendran, R. R. Nivash, P. P. Parthy, and S. Balamurugan, "Modern security threats in the Internet of Things (IoT): Attacks and Countermeasures," in *2019 International Carnahan Conference on Security Technology (ICCST)*, 2019: IEEE, pp. 1-6.
[17]. R. M. Ogunnaike and B. Lagesse, "Toward consumer-friendly security in smart environments," in *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, 2017: IEEE, pp. 612-617.
[18]. E. M. Rudd, A. Rozsa, M. Günther, and T. E. Boult, "A survey of stealth malware attacks, mitigation measures, and steps toward autonomous open world solutions," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 1145-1172, 2016.
[19]. M. M. Ahemd, M. A. Shah, and A. Wahid, "IoT security: A layered approach for attacks & defenses," in *2017 international conference on Communication Technologies (ComTech)*, 2017: IEEE, pp. 104-110.

[20]. S. Shah, S. S. A. Simnani, and M. T. Banday, "A study of security attacks on internet of things and its possible solutions," in *2018 International Conference on Automation and Computational Engineering (ICACE)*, 2018: IEEE, pp. 203-209.

[21]. M. Asplund and S. Nadjm-Tehrani, "Attitudes and perceptions of IoT security in critical societal services," *IEEE Access*, vol. 4, pp. 2130-2138, 2016.

[22]. P. Datta and B. Sharma, "A survey on IoT architectures, protocols, security and smart city based applications," in *2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, 2017: IEEE, pp. 1-5.

[23]. H. Ghadeer, "Cybersecurity issues in internet of things and countermeasures," in *2018 IEEE International Conference on Industrial Internet (ICII)*, 2018: IEEE, pp. 195-201.

[24]. C. Lee and A. Fumagalli, "Internet of things security-multilayered method for end to end data communications over cellular networks," in *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*, 2019: IEEE, pp. 24-28.

[25]. S. Narang, T. Nalwa, T. Choudhury, and N. Kashyap, "An efficient method for security measurement in internet of things," in *2018 International Conference on Communication, Computing and Internet of Things (IC3IoT)*, 2018: IEEE, pp. 319-323.

[26]. I. Ullah, M. A. Shah, A. Wahid, and A. Waheed, "Protection of enterprise resources: A novel security framework," in *2017 International Conference on Communication Technologies (ComTech)*, 2017: IEEE, pp. 98-103.

[27]. N. Gupta, V. Naik, and S. Sengupta, "A firewall for internet of things," in *2017 9th International Conference on Communication Systems and Networks (COMSNETS)*, 2017: IEEE, pp. 411-412.

[28]. C. Liu, Y. Zhang, Z. Li, J. Zhang, H. Qin, and J. Zeng, "Dynamic defense architecture for the security of the internet of things," in *2015 11th International Conference on Computational Intelligence and Security (CIS)*, 2015: IEEE, pp. 390-393.

[29]. S. Sridhar and S. Smys, "Intelligent security framework for IoT devices cryptography based end-to-end security architecture," in *2017 International Conference on Inventive Systems and Control (ICISC)*, 2017: IEEE, pp. 1-5.

[30]. Y. Zheng, S. S. Dhabu, and C.-H. Chang, "Securing IoT monitoring device using PUF and physical layer authentication," in *2018 IEEE International Symposium on Circuits and Systems (ISCAS)*, 2018: IEEE, pp. 1-5.

[31]. M. Ahmad, M. A. Farid, S. Ahmed, K. Saeed, M. Asharf, and U. Akhtar, "Impact and detection of GPS spoofing and countermeasures against spoofing," in *2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*, 2019: IEEE, pp. 1-8.

[32]. P. Zhang, S. G. Nagarajan, and I. Nevat, "Secure location of things (SLOT): Mitigating localization spoofing attacks in the Internet of Things," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 2199-2206, 2017.

[33]. U. Saxena, J. Sodhi, and Y. Singh, "Analysis of security attacks in a smart home networks," in *2017 7th International Conference on Cloud Computing, Data Science & Engineering-Confluence*, 2017: IEEE, pp. 431-436.

[34]. R. J. Robles, T.-h. Kim, D. Cook, and S. Das, "A review on security in smart home development," *International Journal of Advanced Science and Technology*, vol. 15, 2010.

[35]. M. A. Razzaq, S. H. Gill, M. A. Qureshi, and S. Ullah, "Security issues in the Internet of Things (IoT): a comprehensive study," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 6, p. 383, 2017.

[36]. R. Vrooman, "Enhancing Privacy in Smart Home Ecosystems Using Cryptographic Primitives and a Decentralized Cloud Entity," 2017.

[37]. T. Adiono, B. Tandiawan, and S. Fuada, "Device protocol design for security on internet of things based smart home," *International Journal of Online and Biomedical Engineering (iJOE)*, vol. 14, no. 07, pp. 161-170, 2018.

[38]. J. Deng, R. Han, and S. Mishra, "Countermeasures against traffic analysis attacks in wireless sensor networks," in *First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05)*, 2005: IEEE, pp. 113-126.

[39]. D. Desai and H. Upadhyay, "Security and privacy consideration for internet of things in smart home environments," *Int J Eng Res Dev*, vol. 10, no. 11, pp. 73-83, 2014.

[40]. A. Modarresi and J. Symons, "Technological heterogeneity and path diversity in smart home resilience: A simulation approach," *Procedia Computer Science*, vol. 170, pp. 177-186, 2020.

[41]. L. a. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, "IoT Privacy and security: Challenges and solutions," *Applied Sciences*, vol. 10, no. 12, p. 4102, 2020.