IMPROVE SECURITY IN SMART CITIES BASED ON IOT, SOLVE CYBER ELECTRONIC ATTACKS WITH TECHNOLOGY BY USING PACKET TRACER

Raed Al-hamarneh

Computer and Information System Department,
University of Almaarefa, Riyadh, Kingdom of Saudi Arabia

ABSTRACT

Smart cities are expected to significantly improve people's quality of life, promote sustainable development, and enhance the efficiency of operations. With the implementation of many smart devices, c problems have become a serious challenge that needs strong treatments, especially the cyber-attack, which most countries suffer from it.

My study focuses on the security of smart city systems, which include equipment like air conditioning, alarm systems, lighting, and doors. Some of the difficulties that arise daily may be found in the garage. This research aims to come up with a simulation of smart devices that can be and reduce cyber attach. Use of Cisco Packet tracer Features Simulated smart home and c devices are monitored. Simulation results show that smart objects can be connected to the home portal and objects can be successfullymonitored which leads to the idea of real-life implementation and see. In my research make manysolutions for attachingissues,which was great, and apply some wirelessprotocol.

KEYWORD

Smart cities, smart devices, security issue, cyber-attack, Cisco Packet tracer, Cisco Packet tracer

1. INTRODUCTION

In recent times, with the challenges of the modern age and the increasing percentage of pollution, the government began to think seriously about building smart cities with advanced and identical smart specifications, and the main axis was to protect them, from cyber-attacks.

The Internet of Things (IoT) is themain component of information technologies and Internet applications, To connect with smart devices used in daily life via the Internet are the basic concepts. Data from the physical world collected by devices attached to each object is processed andanalyzed and finally used to perform the actions. IoT has covered many areas, such as the health caredomain, smart home, smart transportation, infrastructure management, etc.[1]

Smart city usedsmart devices are typically installed all over the smart city; they can be found everywhere (e.g. streets, stores, residential buildings, elevators, etc.) ,and special smart devices inside houses and offices. However, Citizens may choose to install surveillance cameras and other similar devices in their homes and businesses. This implies that any effort to compromise the smart city's security would be detected, and if a crime was committed, it would be simple to identify the perpetrator. This also indicates that relying on OSINT (short for open source intelligence), which refers to the capacity to collect intelligence information from lawful, open

sources available on electronic systems and massive computers, may be predicted and hence prohibited. [2]

In 2021 Malicious applications that encrypt — and often steal — sensitive data continued to be a top cybersecurity threat 2021. According to a report from the CyberSource provider Coalition, ransomware was responsible for 41% of all CyberSource claims this year.

To learn more about a variety of cybersecurity topics, drop in for a free security webinar.

- 95% of cybersecurity breaches are caused by human error. (Cybint)[3]
- The worldwide information security market is forecast to reach $170.4 billion in 2022. (Gartner)[3]
- 88% of organizations worldwide experienced spear-phishing attempts in 2019[3].
- 68% of business leaders feel their cybersecurity risks are increasing[3]. (Accenture)
- On average, only 5% of companies' folders are properly protected.[3] (Varonis)
- Data breaches exposed 36 billion records in the first half of 2020.[3] (RiskBased)
- 86% of breaches were financially motivated and 10% were motivated by espionage. (Verizon)[3]
- 45% of breaches featured hacking, 17% involved malware and 22% involved phishing. (Verizon)[3]
- Between January 1, 2005, and May 31, 2020, there have been 11,762 recorded breaches. (ID Theft Resource Center)[3]
- The top malicious email attachment types are .doc and .dot which make up 37%, the next highest is .exe at 19.5%. (Symantec)[3]
- An estimated 300 billion passwords are used by humans and machines worldwide. (Cybersecurity Media)[3]

The effective use of advanced technologies (intelligent applications, process digitization, use of UAV resources in combination with information and communication technologies (ICT), real-time data processing and evaluation) in the process management of large and complex systems such as a Smart City is an essential part of building a developed knowledge society. These technologies are effectively employed in the processes of city management, managing limited resources, and meeting stakeholder expectations here [28]

It is feasible to identify 12 important technologies for efficient Smart City administration based on data from Marr and Choudhera. To foster cooperation, data from the field must be collected via the Internet of Things, which is based on the Internet network. After that, the data in the form of Big data is examined. Their long-term viability 5746, 2021, 13, 2021 The amount of confidence in systems and the level of security determine 3 of 20 voluntary sharing. Transparent information supplied through online platforms, dashboards, and models is also essential for increasing public involvement. The trend is now covering the areas of transportation and resource efficiency.[2]

In this study, I will focus on cyber securityissues and how to effectively and professionally reduce it and link it directly through the design of smart, using smart firewall and configurations the server, that denied all attacker, if any hacker break the firewall, other component is hard to crack, thecities and the mechanism of penetration of all kinds and how to treat it using modern methods used in all modern countries of the world.

In my paper will mentation some relate studies in part 2, in part 3 describe smart city and architecture for smart cities and my environments test and discuss the results.

2. RELATED WORK

In the mazing article, the author talks about the use of smart applications has caused many security and privacy issues. The development of more improved protection models and frameworks is critical and in high demand in both corporate and academic settings. This study examined the most recent efforts and advancements in countermeasures from many disciplines' viewpoints..And also discussed up-to-date issues and openchallenges that have emerged in recent years to lay a foundation for further studies. [4]

A recent article,authors Abbas Shah Syed and others present a broad coverage of the Internet of Things in Smart Cities. Supporting a deep discussion of Smart Cities, they present IoT as a vital enabler of smart city services. They talk about security and privacy issues faced by IoT-based Smart Cities are discussed and SWOT analysis. [5]

One of the most beautiful professional works of the author, Chen Ma, was the most prominent role of scanning in explaining intelligent cybersecuritycities, and a survey of the available literature related to security in that technology. It touches on the four main components of a smart city, i.e., smart grid, smart building, Intelligent transportation system, intelligent healthcare. A summary of two methods of deep learning and cybersecurity programs as well as technology connectivity in smart cities. Moreover, the author emphasized the existence of effective functional solutions in maintaining cybersecurity in smart devices, and his study was in-depth in finding solutions to cybersecurity problems, and facing these challenges depends on finding strategic solutions and stimulating the hard work of governments [6]

The author creates in this paper by taking advantage of updates in information technology and networks, the concept of smart cities develops many potential benefits such as improved energy efficiency, management, and personal security. However, this reliance on ICT also makes smart cities vulnerable to cyber-attacks. In this paper, the writer discussed the topic of cybersecurity for smart cities. We explain how specific characteristics of smart cities give rise to cybersecurity challenges, and review the different threats they face. The writer mentioned some of the proposed solutions for cyber security in the form of strategies and analysis. [7]

One of the most challenging papers in front of the current reality that will be very close to my paper is my scientific research where the author mentioned the three layers structure of the Internet of Things and presents the smart home founded on the Internet of things with its benefits and components. In the smart home, it is one of the most important types of big public data analysis. Implementation is discussed to understand the process of data analysis in the smart home. It also poses challenges in ethical areas, especially data security and privacy. Among the topics mentioned by the author is how to protect the three layers and mention the types of intrusions and privacy that must be preserved.[8]

In this brilliant paper, the author makes an in-depth study of smart security in smart cities that are exposed to cyber-attacks. Strangely, smart city technologies are used as a decisive and powerful method of attacks, yet they paradoxically create new risks, including making city infrastructure and services inaccessible Safe, fragile, and open to wide forms of sabotage, disruption and criminal exploitation. The author identified five forms of vulnerabilities and discussed cyber-attacks on city infrastructure and services, citing several illustrative examples where, as far as is known, the majority of attacks are currently repelled using cybersecurity software tools and management practices. Smart cities today have many weaknesses and that these will be exploited for different purposes.[9]

One of the notable reports, in which the author discusses for the first time on the smart city the future of advanced digital life, and how to use three core components - digital technologies, data and design thinking - to enhance and improve services for city residents. However, the writer discussed the digital revolution with digital transformation that also brought new cyber risks that could fundamentally affect the existence of smart cities. Cyberattacks targeting data and physical assets have exploded in recent years, with linked devices growing when speed is compromised - and the number of IoT devices is anticipated to climb from 8.4 billion now to over 20 billion by 2020[10]

The writer emphasized that smart cities are a complex ecosystem of municipal services and public and private entities. The people, processes, devices, city, and infrastructure constantly interact with each of them else. Core Technology Infrastructure The ecosystem consists of three layers: the edge, The core channel and communication The edge layer consists of devices such as sensors, gamers, other IoT devices, and smartphones.[10]

The author discussed several vital topics that talk about smart cities from important components that are available and their function is constantly exchanging data and facilitating the improvement of living for city residents. The paper talks about four main components, which are smart networks, building automation systems (BAS), unmanned aerial vehicles (UAVs), and smart vehicles. With Internet of Things (IoT) sensors enabled and the cloud platform. With the increase in the development of the digital smart system and the increasing of cyber-attacks, when exposed to a cyber incident that includes essential components of the smart city infrastructure, appropriate measures can be taken to identify and enumerate tangible evidence to facilitate the criminal investigation process. Forensic preparedness and lessons learned from past forensic analyzes can help protect a smart city from future incidents. This paper provides a comprehensive view of the security landscape of the smart city, identifying security threats and providing a deep insight intodigital investigation in the context of the smart city.[11]

3. SMART CITY OVERVIEW

The characteristics of smart cities are closely and strongly linked and considered complementary and essential to the security requirements and challenges that are always presented to cybersecurity, and the protection methods presented will be presented based on special scenarios for various smart applications. To provide smart security for all smart cities and homes, it is necessary to introduce the common characteristics, architecture, and applications of smart cities.

3.1. General Iot Architecture for Smart Cities

To combat the growth of many smart cities, lots oftype architecture was created[12]Nevertheless, there is no uniform IoT architecture that we are aware of. The design described here is based on the well-known three-layer architecture and the widely accepted architecture proposed because the focus of this study is to outline security challenges in smart cities.

Nevertheless, there is no uniform IoT architecture that we are aware of it. The design described here is based on the well-known three-layer architecture and the widely accepted architecture proposed in because the focus of this study is to outline security challenges in smart cities.[13]

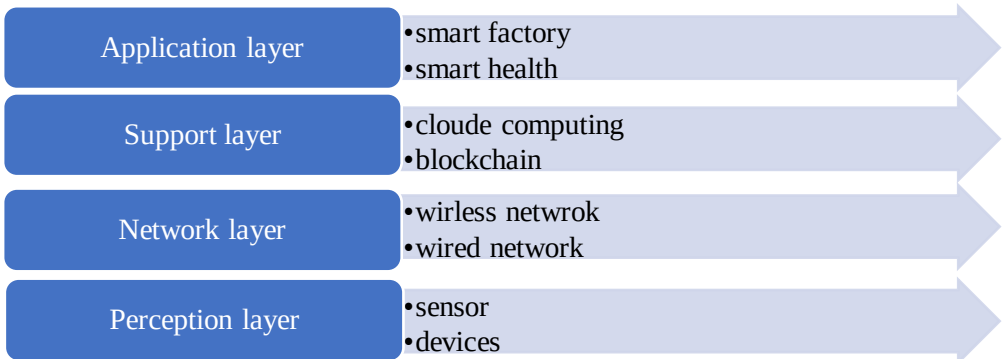

Figure 1. IoT-based architecture for a smart city

In figure 1. The major layers for the IoT architecture are divided into four layers. These are the applicationlayer, service support layer, the network layer and the device layer. At the end layer of the IoT architecture consistsof the physical layer, which is made up of the physical device such as sensors, The second layer is the network layer, which provides the network to connect the smart objectsor "things" to the application layer. The third layer is the service support layer that support servicer and the fourth layer provides the platform for the IoT application service to run. A detail descriptionof each phase of the IoT architecture is discussed below:

- **Application layers**

Is the high some paper called application and transport, HTTPresponsible to sends a message over HTTP utilizing TCP in the application and transport layers. To synchronize data packets over the Internet, HTTP will often rely on TCP. However, because of the verbosity and complexity of the HTTP, it is not suited for deployment on limited devices in an IoT network in the case of IoT[14]. That is to say, the complexity of HTTP header presents a challenge for messages to be sent across from one constrain device to another in an IoT network. The Problem will appear because HTTP is unable to efficiently relay messages by the IoT devices, which are self-aware of their environment. The IoT devices, which are constrained will only allow for a small amount of data to flow in a network. HTTP normally relies on TCP to transmit messages across the Internet. It is important to note that data packets may get truncated in the process of using TCP, which is a stateless protocol to transmit messages across the Internet. They utilized Application Protocol (CoAP) has been used in IoT networks to address this issue with constrained nodes. Therefore, the CoAP can be used to overcome these issues of constrained devices by introducing a binary format that will be carried over a UDP. TheCoAP which is a web transfer protocol will allow constrained devices to be able to remotely send messages across on the Internet and it can also work with HTTP.[15]

- **Support layer**

It is directly related to the application layer, which caters to a wide range of requirements. applications made possible by intelligent computing approaches (e.g., cloud computing) computing)."It will need processing to further decrease the data volume before it travels to the data center or cloud," Jahnke writes. Data can be preprocessed near to the device at the network edge, which may include analytics. Machine learning techniques can be used to offer feedback to the connected system based on telemetry data to enhance its performance.[16]

- **The Network layer**

Is the fundamental layer in the IoT architecture that depends on basic networks, such as the Internet, WANs, and communications networks, The main objects of this layer is to transmit the data collected by the perception layer and to connect smart things, network devices, and servers In IoT design, the network layer acts as the foundation for connecting smart objects in the IoT environment and transmitting data created by devices that are accessible at the application layer. There are many devices in the Internet of Things that are supposed to be uniquely accessible via their IP addresses. IPv4 and IPv6 are the two most common Internet protocols. IPv4 has run out of address space, necessitating the adoption of IPv6, which has a far larger address space to accommodate the billions of IoT devices. TCP/IP is responsible for routing data packets from a source to a destination on the Internet. The Internet works by using the Border Gateway Protocol (BGP), which is an inter-domain protocol that makes use of path-vector routing to send traffic

- **Perception layer**

The lowest layer of the architecture, also known as the sensing layer, physical layer. The perception layer is primarily responsible for gathering data from real-world objects (e.g., heterogeneous devices, WSNs, and sensors) and sending it to the network layer for further processing.

3.2. Main Component of Smart City

One goal of smart city development is to benefit inhabitants in several areas that are strongly connected to their living standards, such as energy, environment, industry, lifestyle, and services. in Fig. 2 and describe them in detail as follows

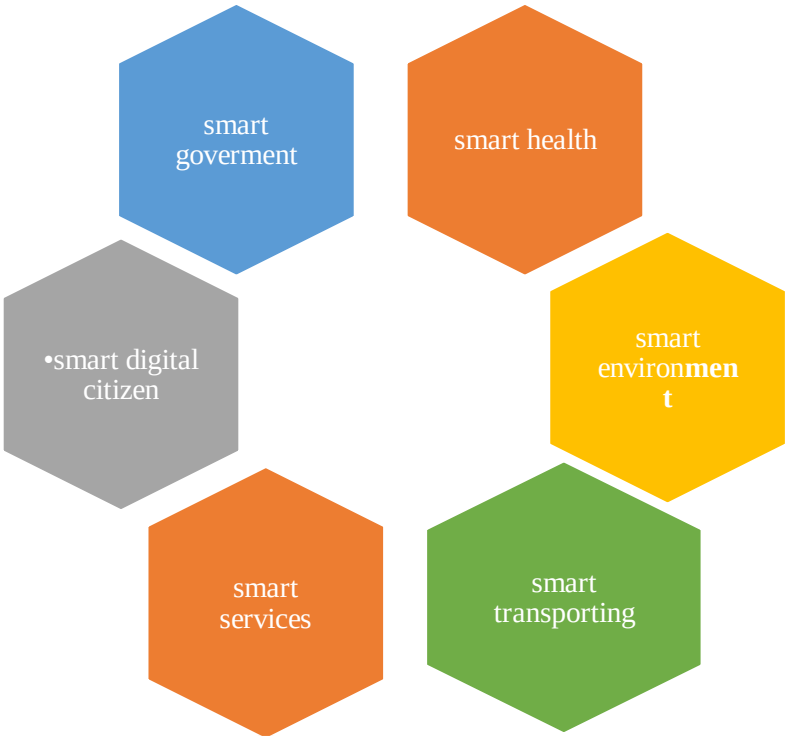

Figure 2. Application in smart city

- **Smart Government**

It is concerned with the use of technology to aid and assist improved planning and decision-making. It's all about enhancing democratic procedures and changing how government services are delivered. E-government, the efficiency agenda, and mobile working are all included.[17]

- **Smart health**

Smart health IT is an open, standards-based technology platform that allows developers to design apps that work throughout the healthcare system smoothly and securely. Patients, doctors, and healthcare practitioners can utilize this library of applications to enhance clinical treatment, research, and public health by using an electronic health record (EHR) system or data warehouse that supports the SMART standard.[18]

- **smart digital citizen**

A digital citizen is someone who participates in society, politics, and government via the use of information technology (IT). Digital citizens are "people who utilize the internet consistently and successfully," according to Karen Mossberger, one of the writers of Digital Citizenship: The Internet, Society, and Participation [19]

- **smart environment**

Smart environments can allow people to engage and interact with their immediate surroundings in a natural and seamless manner. The development of sophisticated technology, along with software-based services, has made this feasible. It is undeniable that technological advancements have ushered in a new age for both sensing and computational processing, allowing for the creation of smart surroundings.[20]

- **smart transporting**

The integrated use of contemporary technology and management methods into transportation networks is referred to as "smart transportation. “You’re probably more aware of it than you realize! Smart transportation might simply refer to the fundamental management systems with which we are already familiar. Such as Car navigation, traffic signal control systems, Automatic number plate recognition, and Speed cameras [21]

- **smart services**

Smart services are digital services that use data of physical products to create value for users like automatic reordering of consumables. New capabilities of technical systems enable smart services and changing business models like pay-per-use require smart services. The reference architecture considers both and supports the planning of new services around an existing product of manufacturing companies.[22]

- **smart utilizes**

Gas, electric, and water utilities that use linked sensors across their grids to assess operations and improve service delivery efficiency are known as smart utilities. To optimize company operations, smart utilities use the Internet of Things (IoT) strategy to link all devices and integrate new digital technology.[23]

3.3. Security Requirements of Smart City:

- **Authentication**

Its a basic requirement for different layers of a smart system and is needed to prove and ensure that only authorized clients can access services across a heterogeneous system Especially, IoT devices deployed in smart cities can authenticate the network, other nodes, andthe messages from management stations. Furthermore, sincethe quantity of authentication data is growing explosively insmart cities, it is important to develop advanced technologiesto guarantee real-time and precise authentication.

- **Confidentiality**

The goal of confidentiality is to prevent information from being disclosed to the incorrect source or being passively attacked. Attackers are expected to be able to eavesdrop on communication or gain access to devices in IoT-based applications. As a result, encryption-based technologies are extensively used to create trustworthy communication and storage systems to secure the secrecy of information transfer between nodes.

- **Availability**

that devices and services should be available when needed. Corresponding to our topic, smart systems or applications should have the ability to maintain effective functioning even when under attack. Moreover, since these devices are susceptible to attacks, a smart system must be able to detect any abnormal conditions and have the ability to stop further damage to the system. Resilienceis regarded as the attack-resistance ability of a system that can tolerate various faults and failures caused by attacks and large-scale disasters. Protection mechanisms should have strong robustness and the ability to continue learning adaptively to cope with the increasingly intelligent attacks

- **Privacy Protection**

Privacy and security are inexorably tied; any of the above requirements might have an impact on privacy protection.it is necessary because it covers various security requirements that were not covered in earlier subsections.

3.4. Security Challenges in IoT Environments (Smart City) and Solution

Smart is a very appealing notion, and a study of comparable studies was carried out to better grasp its principles and design. Cisco packet tracer was utilized for the implementation of the smart city by the majority of researchers.

The Cisco version was chosen because it offers smart city security elements as well as providing a programming environment in addition to networking capabilities. Visual basic, java scripts, and python are among the programming languages supported. Devices like smart windows, smart fans, smart trash, and sensors are controlled via a smartphone and a home gateway. The IOT home gateway ports are linked to the smart devices, and the smart phone is used to interact with them.:

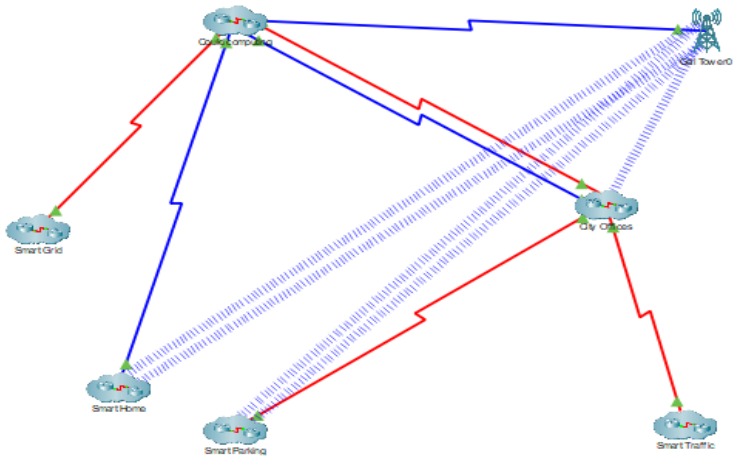

Figure 3. Methodology of the smart city Design [24]

- **Cloud computing:**

in this component, is very important must be secure, so Iinstall firewall5505 and start configuration device for more protection. In cyber security responsible of all follow any attack in figure5

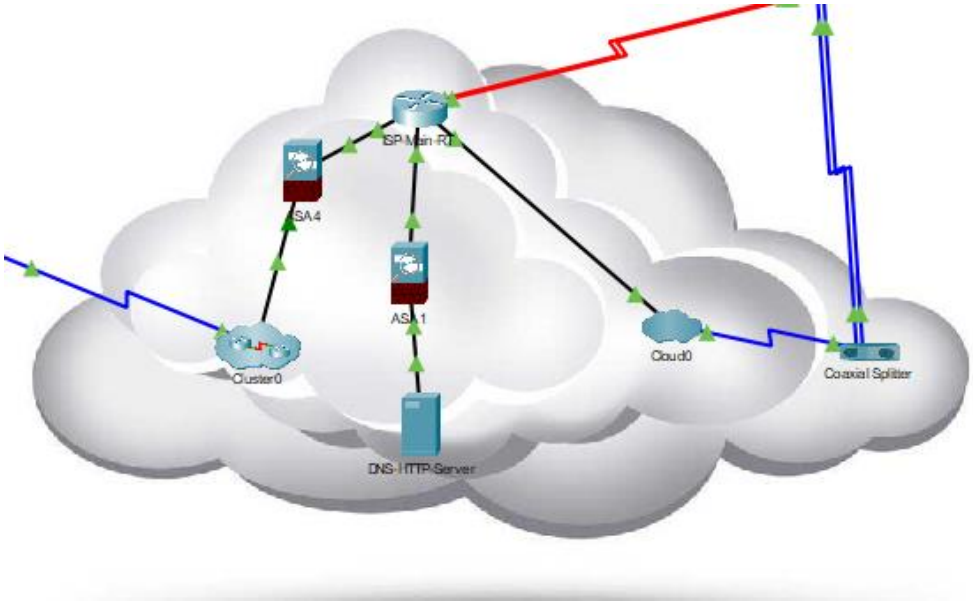

Figure 4. install Two firewall5505

- **Smart Grid**: many solutions for cyberattack next table will discuss:

Smart grid architecture should have suitable and stringent security mechanisms in place to ensure greater security. All devices, meters, components, and communications must have strong authentication and cryptographic architecture (Public Key Infrastructure) technology is a good

way to make a smart grid system more secure. When it comes to smart grid systems, PKI comes in handy.

Solution of the cyber attacker:

- PKI Standards help to establish requirements of security operations of energy service providers such as utilities, generators, smart grid device manufacturers
- Smart Grid PKI Tools is employed to make the easier implementation of PKI in smart grid
- Device attestation is used to define or discover devices and their true identities on the network
- Trust Anchor Security is used to manage trust relationships. Because of having a huge number of devices in the smart grid, an effective and comprehensive Trust Anchor Mechanism System is also needed.

Smart home: This Figure 6 show the simulation of the smart home with cisco packet tracer using the

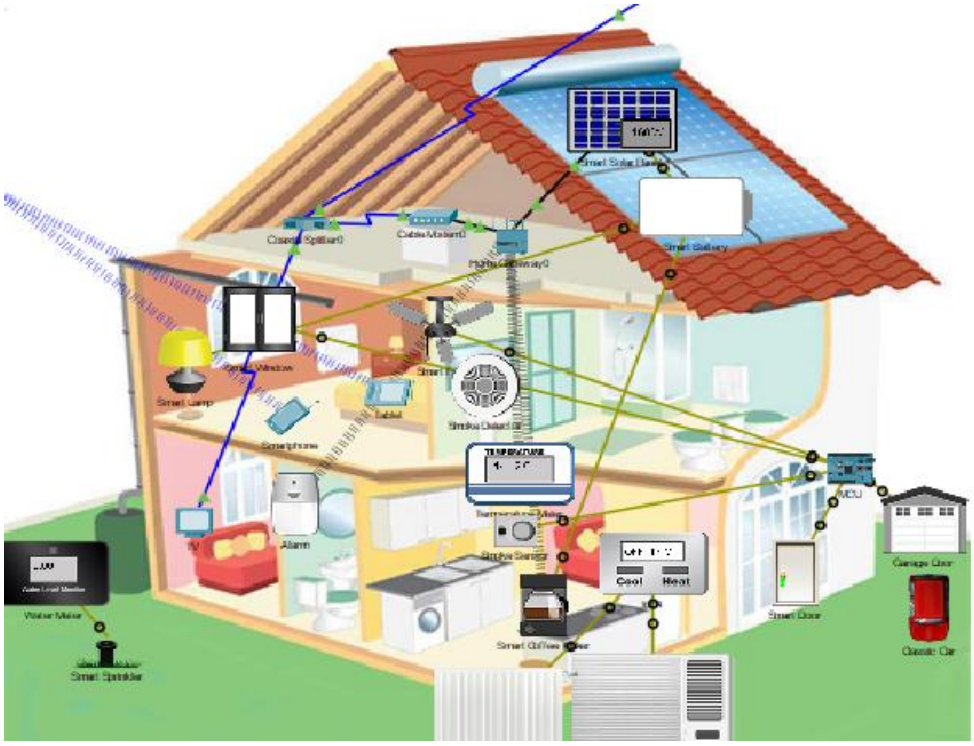

Figure 5. The smart home

Methodology described in the previous page. Home gateway, cloud, ISP (internet service provider) router, central office server, IoT Server, cell tower, smartphone and the car play an important role in the simulation.

Smart home gadgets provide hackers with even more information than the contents of your refrigerator via the linked network. It's also conceivable that IoT devices get hacked and used maliciously without your knowledge. Then take the measures below to keep your smart gadgets safe.

- Consider the risks vs the rewards. [25]
- Create a safe wireless network. [25]
- Don't overlook the significance of your passwords. [25]
- Every new gadget should be registered with the manufacturer and kept up to date [25].
- Consider hiring a pro to do the job. [25]
- Disconnect any gadgets that aren't in use. [25]
- Before discarding gadgets, perform a factory reset. [25]

Smart City office: the consist of (IT Department (cybersecurity, Police department, watching room, other office e-services): One of the most important sections of cyber security has some sensitive matters as it follows up all operations inside the smart city and has a set of precise cyber operations.

- Topology Discovery
- OS Fingerprinting
- Service Discovery
- Packet Capture
- Log Review
- Router/Firewall ACLs Review
- E-mail Harvesting
- Social Media Profiling
- Social Engineering
- DNS Harvesting

- **Smart parking:**Smart parking systems are a critical component of "smart city" concepts, especially in the Internet of Things age (IoT). They wish to relieve the stress of seeking a parking spot in city centers, which has grown increasingly difficult as the number of cars on the road has increased, particularly during peak hours. The following table will examine [2].

Table 1. summary of cyber attach and solution [2]

Attack	Solution
Phishing Attacks	Both the client and the broker use their X.509 certificates to authenticate each other. As a consequence, the broker may verify the client's identity and vice versa without requiring any credentials.
. Man-in-the-Middle (MITM) Attacks	A trustworthy CA issues and verifies certificates that are exchanged between a client and broker. Because we assume that this CA is reliable and safe, the certificates that it issues can be used to verify the authenticity of communications transmitted by the certificate's owner. As a result, to prevent both sides of the MITM attack, our architecture depends on mutual authentication.
Replay Attacks	TLS is used in our proposed architecture to provide a secure communication channel between two parties. As a result, no one can listen in on any section of the conversation. This makes it possible for our architecture to withstand replay assaults.
Broker Hijack	TLS is used in our proposed architecture to provide a secure communication channel between two parties. As a result, no one can listen in on any section of the conversation. This makes it possible for our architecture to withstand replay assaults.

- **Wireless security**

Information is shared among authorized users through wireless networks, however, because to the broadcast nature of the wireless medium, this process is exposed to a variety of malicious attacks. Wireless network security standards are defined to protect wireless communications against wireless attacks such as eavesdropping, denial of service (DoS), data fabrication, node compromise, and so on. [25][26]

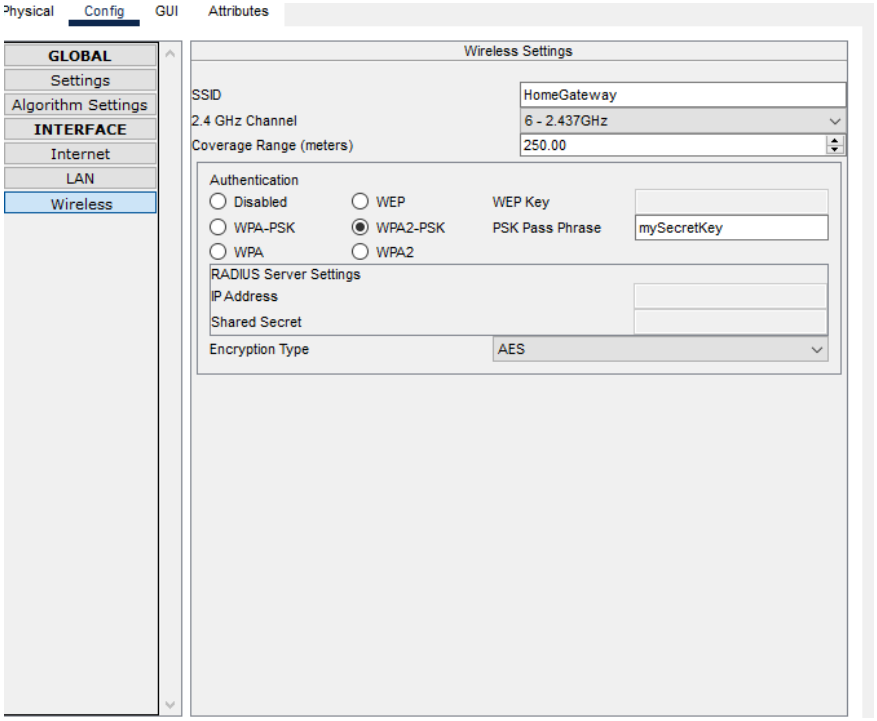

Figure 6. The security configuration of Home Gateway0

3.5. Experimental Results and Analysis

In the simulation, I used packet tracer version 7 usingThe internet of things devices in the Cisco Packet tracer can be used to build and simulate different internet of things applications such as smart home, smart industry, smart office etc. The benefit of using cisco packet tracer is that, user can interact with the devices the same way they do in the real devices. In addition, with it multiuser functionality, multiuser can work together to build virtual network through a real network, I add two firwall : two firewall 5505 component and configuration to be more secure all smart city in figure 5 , ping from the office , is work done , other ip address not work

```
A5505(config)# show log
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Standby logging: disabled
    Debug-trace logging: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: level debugging, 39925 messages logged
    Trap logging: disabled
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: disabled
n" [0x0, 0x0]
%ASA-4-106023: Deny tcpsrc inside:10.71.0.50/54843 dst
outside:10.0.0.10/445 by access-group "inside-in" [0x0, 0x0]
%ASA-4-106023: Deny tcpsrc inside:10.71.0.50/54845 dst
outside:10.0.0.10/445 by access-group "inside-in" [0x0, 0x0]
%ASA-4-106023: Deny tcpsrc inside:10.71.0.50/54844 dst
outside:10.0.0.10/445 by access-group "inside-in" [0x0, 0x0]
%ASA-4-106023: Deny tcpsrc inside:10.71.0.50/54850 dst
outside:10.0.0.10/139 by access-group "inside-in" [0x0, 0x0]
%ASA-4-106023: Deny tcpsrc inside:10.71.0.50/54843 dst
outside:10.0.0.10/445 by access-group "inside-in" [0x0, 0x0]
%ASA-4-106023: Deny tcpsrc inside:10.71.0.50/54845 dst
outside:10.0.0.10/445 by access-group "inside-in" [0x0, 0x0]
%ASA-4-106023: Deny tcpsrc inside:10.71.0.50/54844 dst
outside:10.0.0.10/445 by access-group "inside-in" [0x0, 0x0]
%ASA-4-106023: Deny tcpsrc inside:10.71.0.50/54850 dst
outside:10.0.0.10/139 by access-group "inside-in" [0x0, 0x0]
%ASA-4-106023: Deny udpsrc inside:10.71.0.50/137 dst
outside:10.0.0.10/137 by access-group "inside-in" [0x0, 0x0]
%ASA-6-302014: Teardown TCP connection 4718 for
outside:173.194.40.49/443 to inside:10.71.0.50/54803 duration 0:02:00
bytes 1554462 TCP FINs
```

Figure 7. access denied IP address only determine in my configuration

In smart home , Figure 7 I add WAP2-PSK for authorized person , in smart phone I add all IoT devices as in Figure 9, other area , smart parking or office the packet tracer have limitation in IOT

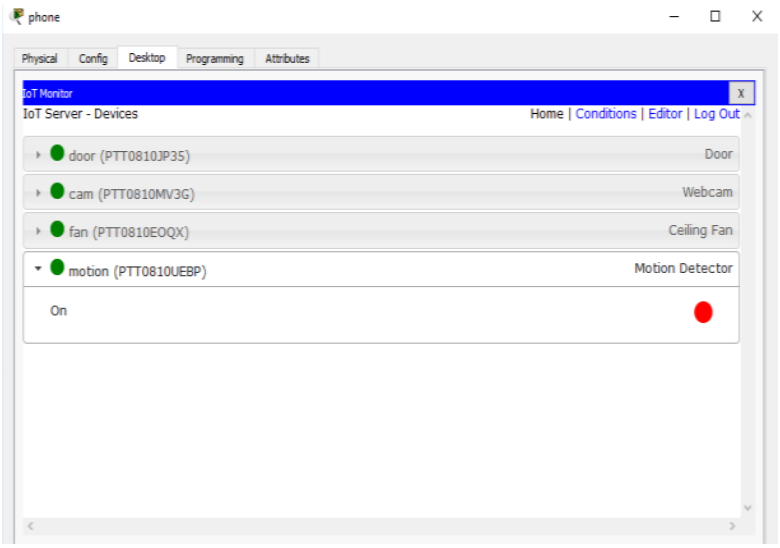

Figure 8. Smart Add all smart IoT in his mobile

4. CONCLUSION AND FUTURE WORK

Configuring the server and the smart firewall has a tremendous and tremendous ability to prevent electronic intrusion, regardless of the hacker's ability to access the server and even all the rest of the components. Here was the take-off and even my paperwork only focused on how to simulate the Internet of Things using the Cisco packet tracer, so any research on other IoT simulators in this study has been done with more protections in cybersecurity, meeting all the challenges in cybersecurity across the board Smart parking. Since then Cisco is expected to release a new version of the packet tracer with more IoT devices, and more complex IoT applications can be simulated in the future.

This distinguished practical paper that attempts to prevent electronic intrusions at the cost of methods and with the existence of wonderful, amazing, and amazing technical solutions, with the presence of these modern technologies, the cyber penetration has a strong imprint in the old-time, but now the beginning of the demise and the start of the safe Internet, which we will touch soon during the coming years

ACKNOWLEDGMENT

The author would like to thank Al Maarefa University for the financial support of this research.

REFERENCES

[1] M. R. R. A. K. B. &. K. B.-S. Burhan, "IoT Elements, Layered Architectures and Security," IoT Elements, Layered Architectures and Security, pp. 1-37, 2018.

[2] A. Ali ,, I. Alrashdi1, , E. Aloufi1, , M. Zohdy2, H and . H. Ming1, "SecSPS: A Secure and Privacy-Preserving," Journal of Information Security, vol. 9, pp. 299-314, 2019.

[3] R. Sobers, "134 Cybersecurity Statistics and Trends for 2021," varnonis, 2021 6 3. [Online]. Available: https://www.varonis.com/blog/cybersecurity-statistics/. [Accessed 4 9 2021].

[4] G. X. Y. LEI CUI, "Security and Privacy in Smart Cities:," IEEE ACCESS, no. SPECIAL SECTION ON CHALLENGES AND OPPORTUNITIES OF BIG DATA AGAINST CYBER CRIME, 2018.
[5] D. S.-S. K. E. Abbas Shah Syed, "IoT in Smart Cities: A Survey of Technologies,Practices and Challenges," MDPI , vol. 4, p. 429–475, 2021.
[6] C. Ma, "Smart city and cyber-security; technologies used, leading challenges," Energy Reports, 2021.
[7] R. A. J. Z. A. Armin Alibasic, "Cybersecurity for Smart Cities: A Brief Review," 2017.
[8] "Smart Home based on Internet of Things and Ethical Issues," Science and Technology Publications, pp. 57-64, 2021.
[9] R. K. a. a. M. Dodgeb, "The (In)Security of Smart Cities: Vulnerabilities, Risks,," JOURNAL OF URBAN TECHNOLOGY, vol. 26, p. 47–65, 2019.
[10] P. PANDEY, "Making smart cities cybersecure," Deloitte Insights, USA, 2019.
[11] Z. A. Baig, C. Valli, P. Rabadia, P. Hannay,, M. Chernyshev, M. Johnstone, P. Kerai, A. Ibrahim and K. Sansurooah, "Future challenges for smart cities: Cyber-security and digital forensics," Digital Investigation, Australia, 2017.
[12] I. Y. e. al., "Internet of Things architecture: Recent advances, taxonomy,," IEEE Wireless Commun., vol. 24, pp. 10-16, 2017.
[13] L. T. a. N. Wang, "Future Internet: The Internet of Things," computer Theory, vol. 5, pp. 376-380, 2010.
[14] A. Castellani, L. Vangelista, and M. Zorzi,, "Internet of Things for Smart Cities," IEEE INTERNET OF THINGS JOURNAL, vol. 1, 2017.
[15] K. H. C. B. a. B. F. Z. Shelby, "Constrained application protocol (CoAP)," 2018. [Online]. Available: http://tools.ietf.org/html/draft-ietf-corecoap-.
[16] P. Godstin, "What Is IoT Architecture, and How Does It Enable Smart Cities?," 16 6 2021. [Online]. Available: https://statetechmagazine.com/article/2021/06/what-iot-architecture-and-how-does-it-enable-smart-cities-perfcon. [Accessed 17 9 2021].
[17] p. kumar, "CivilsdailyCivilsdaily," 5 11 2018. [Online]. Available: https://www.civilsdaily.com/mains/what-do-you-mean-by-smart-governance-highlight-its-significance-in-the-context-of-indian-bureaucracy-150w-10m/. [Accessed 18 9 2021].
[18] "What Is SMART?," smart, 15 9 2018. [Online]. Available: https://smarthealthit.org/an-app-platform-for-healthcare/about/. [Accessed 9 19 2021].
[19] "Digital citizen," From Wikipedia, the free encyclopedia, 4 7 2019. [Online]. Available: https://en.wikipedia.org/wiki/Digital_citizen. [Accessed 19 9 2021].
[20] W. B. C.D. Nugent, "Smart Environment," Journal of Network and Computer Applications, 2017, 2016.
[21] M. Michel, "what is Smart Transportation and is it the Future?," 2019. [Online]. Available: https://blog.gunneboentrancecontrol.com/what-is-smart-transportation-and-is-it-the-future. [Accessed 19 9 2021].
[22] M. Rabe, L. Asmar, A. Kühn and R. Dumitrescu , "PLANNING OF SMART SERVICES BASED ON," INTERNATIONAL DESIGN CONFERENCE, p. 2949, 2018.
[23] virtusa, "Smart Utilities," 2021. [Online]. Available: https://www.virtusa.com/digital-themes/smart-utilities. [Accessed 19 9 2012].
[24] cisco, "csic network acadmey," 2021. [Online]. Available: https://www.netacad.com/ar. [Accessed 23 9 2021].
[25] D. M. a. G. Tsudik, "Security and privacy in emerging wireless network," IEEE Wireless Commun, vol. 17, pp. 12-21, 2010.
[26] D. S. a. A. K. H. Kumar, "threats in wireless sensor networks," Aerosp. Electron. Syst. Mag, vol. 23, pp. 39-45, 2008.
[27] R. D. Steele, The Millennium Development Goals Report (2008), 2008. [Online]. Available: http://www.un.org/millenniumgoals/pdf/MDG%20Gap%20Task%20Force%20Report%202008..
[28] Y. Qing and Qang, "L. Resource Scheduling and Strategic Management of Smart Cities under the Background of Digital Economy.," 2020.