Journal of Engineering Sciences and Information Technology
Volume (5), Issue (3): 30 Sep 2021
P: 112 - 133

ISSN: 2522-3321

مجلة العلوم الهندسية وتكنولوجيا المعلومات
المجلد (5)، العدد (3): 30 سبتمبر 2021م
ص: 112 - 133

Predicting Internet of Things (IOT) Security and Privacy Risks – A Proposal Model

Awad Saad Al-Qahtani

Mohammad Ayoub Khan

College of Computing and Information Technology || Bisha University || KSA

Abstract: The Internet of things (IOT) users lack awareness of IOT security infrastructure to handle the risks including Threats, attack and penetration associated with its use. IOT devices are main targets for cyber-attacks due to variable personally identifiable information (PII) stored and transmit in the cyber centers. The security risks of the Internet of Things aimed to damage user's security and privacy. All information about users can be collected from their related objects which are stored in the system or transferred through mediums among diverse smart objects and may exposed to exposed dangerous of attacks and threats if it lack authentication so there are essential need to make IOT security requirements as important part of its efficient implementation. These requirements include; availability, accountability, authentication, authorization, privacy and confidentiality, Integrity and Non-repudiation. The study design is a survey research to investigate the visibility of the proposed model of security management for IOT uses, the security risks of IOT devices, and the changes IOT technology on the IT infrastructure of IOT users through answering of the research questionnaires. This work proposes a model of security management for IOT to predict IOT security and privacy threats, protect IOT users from any unforeseen dangers, and determine the right security mechanisms and protocols for IOT security layers, as well as give the most convenient security mechanisms. Moreover, for enhancing the performance of IOT networks by selecting suitable security mechanisms for IOT layers to increase IOT user's security satisfaction.

Keywords: The Internet of things, IOT security, Authentication, privacy

توقع مخاطر أمن وخصوصية إنترنت الأشياء (IOT) – نموذج مقترح بحثي

عوض سعد القحطاني

محمد أيوب خان

كلية الحاسبات وتقنية المعلومات || جامعة بيشة || المملكة العربية السعودية

المستخلص: يفتقر مستخدمو إنترنت الأشياء (IOT) إلى الوعي ببنيته التحتية الأمنية للتصدي للمخاطر بما في ذلك التهديدات والهجوم والاختراق الإلكتروني المرتبط باستخدامه. وتعد أجهزة إنترنت الأشياء أهدافًا رئيسية تستهدفها الهجمات الإلكترونية للوصول إلى معلومات التعريف الشخصية المتغيرة (PII) التي يتم تخزينها ونقلها في المراكز الإلكترونية. كما تستهدف المخاطر الأمنية لإنترنت الأشياء، الإضرار بأمن وخصوصية المستخدمين. ويمكن الوصول إلى جميع المعلومات المتعلقة بالمستخدمين من خلال تلك الأجهزة حيث إن المعلومات مخزنة في النظام أو يسهل نقلها عبر الوسائط بين تلك الأجهزة الذكية المتنوعة، وقد تتعرض لخطر الهجمات والتهديدات الإلكترونية إذا لم تكن مرخصة. وبناءً عليه، يتوجب تطبيق شروط الأمان على إنترنت الأشياء كجزء ضروري ضمن شروط استخدامه. وتشمل هذه الشروط: سهولة الوصول والمسئولية والترخيص والمصادقة والخصوصية والسرية والشفافية وعدم التنصل من المسئولية. ويمثل تصميم الدراسة بحثًا استقصائيًا للتحقق من مدى إمكانية تطبيق النموذج المقترح لإدارة الأمان، على استخدامات إنترنت

الأشياء، والمخاطر الأمنية لأجهزة إنترنت الأشياء، والتطويرات التي أجرتها تقنية إنترنت الأشياء على البنية التحتية لتكنولوجيا المعلومات لمستخدمي إنترنت الأشياء، من خلال الإجابة على استبيانات البحث. ويقترح هذا البحث نموذجًا مقترحًا لإدارة الأمان لإنترنت الأشياء للتنبؤ بالمخاطر التي تهدد أمان إنترنت الأشياء والخصوصية ومن أجل حماية مستخدمي إنترنت الأشياء من أي مخاطر غير متوقعة واختيار آليات وبروتوكولات الأمان المناسبة لمستويات الأمان في إنترنت الأشياء. كما توفر أفضل الخيارات من آليات الأمان المطمئنة. وعلاوة على ذلك، لتحسين أداء شبكات إنترنت الأشياء عن طريق اختيار آليات الأمان المناسبة لمستويات إنترنت الأشياء لتزيد من احتياطات الأمان بما يرضي مستخدم إنترنت الأشياء.

الكلمات المفتاحية: إنترنت الأشياء، مستويات أمان إنترنت الأشياء، المصادقة، الخصوصية.

1. Introduction:

The Internet of Things (IOT) is fast growth and will be targeted for attack, it considers as an internet of threats that it has many challenges include issues with application standardization, scalability, and security and privacy as IOT applications lack communications and data security, (Huawei, 2018). Current encryption methods are built based on the processor speeds and memory of devices such as smart phones, PCs, and tablets, with the restricted memory and processor speed of IOT devices influencing the application of existing encryption techniques, (Chen Long, 2017). Most significant challenges for the Internet of Things is Authentication where biometrics will un able to make IOT devices authenticated, and passwords will be inefficient and unstable due to the large number of devices. Individual privacy is an issue that the individuals may be followed without their permission or understanding, (Jayavardhana et al, 2013). IOT systems are very complicated that it need bidirectional communication and information exchange to be compatible and profitable, (Yasirli et al., 2018). IOT systems are very complicated including edge devices, firmware, protocols, and software with complex configurations where the more complicated system resulted in more difficult to design and implement and uses secure, (Osisanwo et al., 2015). Many IOT devices are easily attacked or penetrated due to weak passwords and lack adequate security controls where According to Hewlett-Packard Development Company, around 70% of the most commonly used IOT devices have penetrated and most of IOT devices collect as one piece of personally identifiable information (PII) Insecure data exploited to improve security of the data and manipulate university systems, (Sharon et al., 2014).

1.1. Study problem:

Most IOT consumers lack the knowledge of IOT security infrastructure necessary to control the hazards posed by the Internet of Things and there are many threats and challenges face the IOT security and privacy IOT users so this study introduce a proposed model for security management of the Internet of Things to face these threats and any unforeseen risks for IOT security and privacy IOT users with introducing an appropriate security mechanisms and protocols for the levels of security in IOT to improve the performance of IOT networks and increase security precautions to the security and privacy IOT users.

1.2. Research questionnaires:

1- Is a proposed Model for Predicting IOT Risks valuable to the IOT industry?
2- Is a proposed Model for Predicting IOT Risks valid technically?
3- What are the Ranking of IOT risks factors in terms of importance as mentioned in a proposed Model?
4- What are the risks estimation techniques can be implemented in a proposed model?
5- Is a proposed Model for Predicting IOT Risks sufficient to protect IOT Users?

1.3. Objectives of the study:

This study introduces the best choices of convenient security mechanisms, which provide security satisfactions to IOT users. This paper suggests a proposed model of security management for IOT to predict IOT security and privacy risks in order to protect IOT users from any unexpected risks and choose the appropriate security mechanisms and protocols for IOT security layers. Moreover, for enhancing the performance of IOT networks by selecting suitable security mechanisms for IOT layers to increase IOT user's security satisfaction.

1.4. Research Significance:

This study is useful for IOT user that by identification the IOT risks, the IOT Users might encounter and can apply the connected devices widely to involve industrial smart manufacturing, medical equipment, home automation, security cameras, door locks, and heating and cooling systems. By identification of challenges of the Internet of things, the IOT Users will prepare for expected new challenges to the Internet of Things. This research examined the impact the IOT on IT security management according to IOT Users and will be introducing a proposed model of security management for IOT. The proposed model will be used to predict IOT security and privacy risks to protect IOT users from any unexpected risks and choose the appropriate security mechanisms and protocols for IOT security layers.

1.5. Chapter Summary:

This research seeks influences of the Internet of Things (IOT) on the IT security and structure. The study design is a survey research to investigate the visibility of the proposed model of security management for IOT uses, risks which faced IOT devices, and the changes of infrastructures and IT of IOT technology through answering of the research questionnaires. The samples represented in the participants who have information technology professionals. This study depends on secondary Data collected and originated from an online survey. Statistical analysis will be used for the results to approve the study objectives. The results of this research included the identification of the types of IOT devices; the identification of the security risks of IOT devices; and the identification of the changes the IOT had on the IT security infrastructure faced IOT users. The data analysis connect between the categories in order to get

conclusions for IOT users deploying IOT devices have the opportunity to increase satisfaction and efficiency. The increase in the number of connected devices enhances the potential attacks.

2. Review of Literature:

2.1. Background:

The term of IOT means growing network of physical objects with IP address for internet connection and the communication among these objects and other Internet- systems. IOT refers to the technologies and research fields that enable the internet to connect with actual objects in the real world. There are two major technologies that precede IOT and similar in functionality; the first technology is Supervisory Control and Data Acquisition (SCADA) which consists of multiple remote terminal units that work as data collectors or sensors, sending information to the main terminal unit. The main terminal unit collects that information and processes it. The second technology is Radio Frequency Identification (RFID) is automatic identification and data capture method that identifies tags attached to objects used to track things in transit or at remote locations. Recently, incorporate intelligence into these IOT devices beyond basic sensing of physical attributes. Terms like a smart car, smart home, and smart fridge are evidence of the incorporation of smartness into these IOT devices, (Maryam et al., 2017). These are some of the important benefits that can be derived from IOT adoption such as; healthcare, smart farming, energy and water consumption monitoring, Smart drones, (Sharon et al., 2013). Most IOT devices incorporate sensors that measure physical attributes. Sensors collect data that are transmitted to either a network node or a control center where a decision is made and a corresponding result is sent back to an actuator in response to the sensed input, IOT can be used to leverage existing technologies like fog and cloud computing, (Abomhara and Køien, 2015).

2.2. Research structure:

2.2.1. Terms and definitions:

All DOD information and accreditation described the fundamental security as assurance pillars

2.2.2. Authentication:

This service seeks to establish that an entity exists. It is typically established by demonstrating the concealed possession of a personal physical item such as a pass ward and/or personal traits such as fingerprints, facial, and iris recognition, (Ferrag et al., 2017).

2.2.3. Confidentiality:

This service seeks to prevent unauthorised parties from accessing the content of stored and transferred data. It is mostly accomplished through the use of encryption techniques, (Abdul Wahab et al., 2017).

2.2.4. Integrity:

This service strives to ensure that the content of data stored or transferred has not been altered, either unintentionally or intentionally., (Mian et al., 2017).

2.2.5. Availability:

This service assures that system services and resources are instantly and continuously available for users, when needed, (El Mouaatamid et al., 2016)

2.2.6. Non-repudiation:

This service makes it impossible for any party involved to deny that any legal or unlawful activity was delivered, received, executed, or modified. Digital signature technology, which is widely utilised in asymmetric cryptography, is usually utilised to deliver it, (El Mouaatamid et al., 2016).

2.2.7. IOT application domains:

2.2.7.1. Smart Home:

Home automation is a recent trend that is gaining attention and one of applications of IOT. It can be used for monitoring of energy and water consumption. It also enables remote control of appliances to regulate lighting and indoor climate. Intrusion detection, access control, and alarm system for home security are other important applications to ensure safety at homes, (Ferrag et al., 2017). Smart home devices typically connect to a central hub or gateway. Some IOT devices are connect to the router over Wi-Fi, while others use device gateway architecture and connect via a smart phone, (Abomhara and Køien, 2015).

2.2.7.2. Smart Cities:

This application domain entails the incorporation of connectivity and intelligence to cities' infrastructure to enhance the quality and performance of urban services to improve the utilities and energy to reduce wastage. One of the IOT devices used in smart cities is Air quality sensors, which helps measure smoke, dust and other particulate air pollution, (Sneha and Bansod, 2012). Smart streetlight is another IOT device used in cities and control by identifying opportunities for improved power usage and optimizing operational efficiency dynamically through the sensors and microcontrollers based on the

weather conditions, time of the day, motion detection, and traffic density by intelligent and remote control, (Abuhasel et al., 2020).

2.2.7.3. Health Care applications:

The application of IOT in health care has enabled remote real-time health monitoring, tracking, and maintenance of assets, new devices are emerging for telemedicine, prognosis, and treatment. Smart inhaler is One of the IOT devices which depend on utilizes Bluetooth technology for connectivity. It can alert patients when to take their medication and gather data for use in evaluating patients' adherence, (Elleithy etal., 2006).

The smart glucometer is another IOT device that helps in diabetes management. Most current smart blood sugar meters use Bluetooth for wireless communication and have a corresponding mobile app, (Atamli and Martin, 2014). Medical IOT devices include smart insulin pen, smart bandages, smart beds, smart scales, smart track, hearables, and ingestible sensors and other notable applications of IOT in healthcare involve fall detection for elderly or disabled people, control of conditions inside medical fridges storing vaccines, and radiation surveillance, all are easy to use and effective for tracking user's health, (Elleithy etal., 2006).

2.2.7.4. Industry applications:

Industrial IOT (IIOT) is used across several industries like manufacturing, oil and gas, energy, mining and aviation. Smart grid is one prominent example of IOT application in the energy sector, smart meter is prominently used at home to record electrical usage. It enables two-way communication via WiFi or ZigBee. Smart water meter is another IOT device used in public water system. It is equipped with a microcontroller which enables direct electronic reading of water consumption and can be controlled over a wireless sensor network, (Farooq et al., 2015). The smart robotics. It is used extensively in assembly or production lines for putting parts together in manufacturing industries. Smart robots are perfect for tasks requiring speed and accuracy. They can help save hours spent on monotonous jobs thus allowing human workers to partake in more creative and sensitive tasks. Recently, IOT has also been applied in aviation industry. Smart sensors used in the aviation facilitates prompt decision making using real time sensor data for time-sensitive processing, (Pallavi & Sarangi, 2017).

2.2.7.5. Transportation applications:

A smart vehicle can employ sensors to monitor driver weariness and mood based on driving conditions, driver behavior, and facial signs to ensure safe driving by triggering warning systems or operating the vehicle directly. Smart parking sensor is one prominent device used in intelligent parking system to visualize and detect the occupancy of parking spaces in real-time. The sensors detect the presence of vehicle and transmit space status information via radio signals to a central server. The

application of IOT in transportation can also help in maintaining vehicle health, curbing traffic congestion and improving fleet logistics, (Suoa et al., 2012).

2.2.7.6. Agriculture applications:

Agricultural automation is another technique that involve the application of robotics, automatic control and artificial intelligence to all levels of agricultural production. Moocall is a wireless calving alert sensors that can detect when a cow is going into active labor. Arable Mark Crop Senor is an IOT device used in crop management. It can be used to measure and predict precise conditions of crops. Climate-smart agriculture is another application for IOT which aim to ensure food security in a changing climate, (Atzori et al., 2010).

2.2.7.7. Retail:

Recent technological advancement and IOT application in retail has witnessed new dimensions of operation to reduce inventory error, optimize supply chain management and decrease labor costs. Intelligent shopping, smart product management and payment processing are other notable applications. One of the devices useful in the integration of IOT technology with retail processes is beacon It is a device that emit radio signals, identifying itself within a location. Moreover, recent technological development in retail have been involved smart store, smart warehouse, smart shelf, (Zhao & Lina, 2013).

2.3. IOT Literature Review:

There are various studies as well as services that have been conducted on the current trends in IOT security. Data security and privacy for IOT devices is still a major problem, and it will be for the foreseeable future. Dhanjani (2013) used website that exploit vulnerability. Java atomic reference array exploit to study DOS attack against Philips Hue light bulb. A recent review examines IOT vulnerabilities, attack vectors, and exploitations the seriousness of IOT issues, hurdles, and expected solutions as reported by)Yassine et al. & Mian et al., 2017). The importance of security protection mechanisms and the ramifications of device vulnerabilities in IOT are further emphasized in a survey that shows techniques used by major IOT communication protocols and analyses some of the attacks against real IOT devices. The surveys discussed with focus on the importance of security protection mechanisms and the ramifications of device vulnerabilities in IOT, as reported by (Abdul Wahab et al., 2017). Kuma et al., 2016 investigated the excessive data and storage solutions that do not consider performance and security by proposing IOT-Discovery Service (DS) to address security issues specifically on distributed data storage access and identification, as well as designing a custom access control model as a fine grain method of controlling data access and utilising two lanes. (El Mouaatamid et al., (2016) presented a warning vulnerability detection algorithm by utilizing attack graph to model vulnerabilities and discusses ways to assess network security in IOT environment, create tactics for detecting and removing high-risk attack

routes, and examines large-scale vulnerability assessments of consumer IoT devices, including the use of Nessus to find potential weaknesses. Yoon et al. (2017) used Remote security management server to improve Security management for IOT Remote.

Naik et al. (2017) provided a holistic definition of IOT harmful behavior, as well as an examination of IOT security concerns.

Kwon et al. (2016) discussed the Security issues on distributed Custom access control data storage access and model identification by using Custom access control model technique.

Farooq et al., 2015, demonstrated the proliferation dangerous of vulnerable IOT devices and the massive DDOS attack on the company, which exploited well-known attack vectors such as default passwords and the outdated Telnet service to take control of millions of web cameras made by a single Chinese manufacturer. Yassine et al., 2017 retrieved hardcoded encryption keys from LIFX brand light bulbs and used them to recover the local network's Wi-Fi password, approving the use of DoS attacks against Philips Hue. The Philips Hue and Limitless Led systems can be used to establish a hidden channel to filter data from air-gapped networks, resulting in strobes that can cause epileptic seizures. George et al. (2018) designed a model in order to remove of high-risk attack pathways for securing IOT networks from vulnerability exploitation. Williams et al. (2017) utilized Nessus vulnerability scanner in large-scale vulnerability assessment. Blythe et al. (2018) extracted data from device user manuals, online surveys for Develop a consumer security index. Gurabi et al. (2018) approved two-factor authentication based on smart card affect user authentication in IOT. Shah et al. (2018) utilized a secure vault in Authentication of IOT devices. Rahman et al., (2016) used Reverse engineering and development of SensCrypt protocol for Vulnerabilities in fitness trackers. Ho et al. (2016) Utilized Touch-Based Intent Communication for Security analysis of smart locks. Costin et al. (2016) utilized a framework that leverages off-the-shelf static and dynamic analysis tools for Firm ware analysis.

Tekeoglu et al. (2014) Test bed setup and network traffic monitoring using port mirroring for Security evaluation of Chrome cast network communication. Fernandes et al., (2016) utilized a computation model and Flow Fence Data to improve protection for IOT frameworks. Jia et al., (2017) utilized open source tools for traffic monitoring, mirrored packet sniffers for Investigating security of cloud- based wireless IP camera.

3. IOT Proposed Model

3.1. Overview

The proposed Model framework consists of four main stages. The first stage is IOT security and privacy risks configuration Data Base, the second stage is an IOT intrusion Risks Detections by scanning

security and privacy risks, the third stage is matching between IOT Risks scanning results with IOT security and privacy risks Data Base. The last stage is IOT interception reports as shown in figure (1).

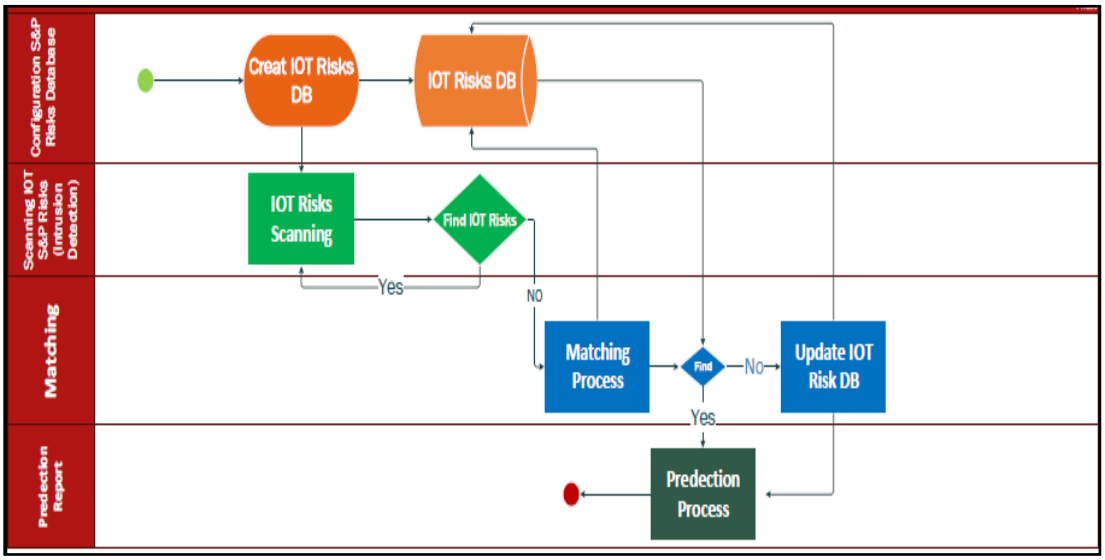

Figure (1) Framework of the four phases of Proposed Model

3.2. Proposed Model Framework:

Model framework as showed in figure (2) consists of 4 phases. Model framework suggests procedures for attack detection algorithms and for performing the routine duties such as reading and sending sensor readings which turn framework's outer layer as a wrapper for the entire application. Another procedure is program that matching between scanning risks results in terms of collecting intrusion values and sending these over the network to find the Risks identification from IOT Risks Data base. The results of matching procedure will be acts as a common IOT Risks reports as an Alarm for users of IOT.

3.2.1. Phase (1): IOT security and privacy risks configuration Data Base:

In this procedure, an IOT risks database will be created, data of IOT risks types will be entered into the database.

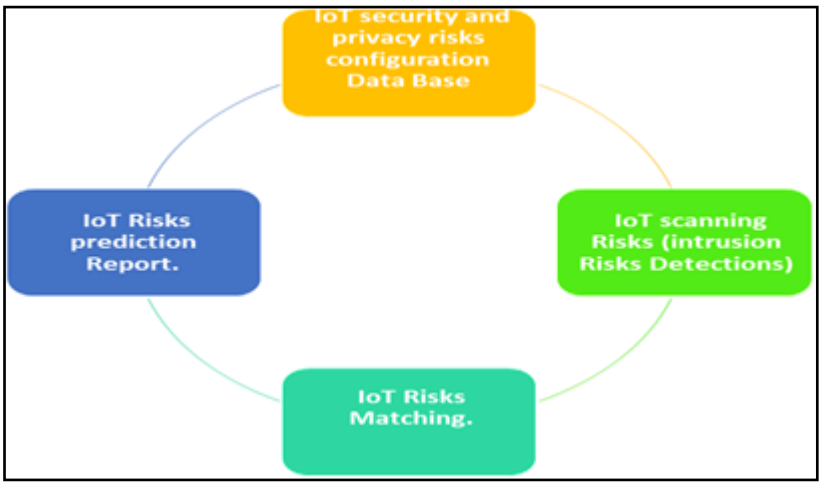

Figure (2) Four phases of Proposed Model

3.2.1.1. IOT Risks classification:

Traditional Internet protocols, which require lightweight protocols to address issues of limited energy, data rate, and computing power, are different from IOT systems, which require lightweight protocols to address issues of limited energy, data rate, and computing power, according to security mechanisms that are used IOT security and privacy risks are classified to authentication, confidentiality, integrity, and availability to authentication, confidentiality, integrity, and availability to authentication, confidentiality, integrity, and availability to authentication, confidentiality, integrity, and availability to authentication, confidentiality, integrity, and availability to authentication, confidentiality, integrity. In the resource-constrained phase of IOT, wireless communication technologies such as Wi-Fi, Bluetooth, ZigBee, and RFID (Radio Frequency Identification) are also beneficial for IOT risk classification.

3.2.1.2. Taxonomy of Wireless IOT Attacks:

Accidental and purposeful risks to the Internet of Things (IOT) exist. If an attack is carried out only utilizing information technology tools, such as a cyber attack, it can be characterized as either an insider or an outsider attack. Outsiders are generated by person from outside the network, such as a hacker, in the current study. The four security services that be compromised in attacks are authentication (fabrication), confidentiality (interception), integrity (modification), and availability (interruption). This dominance class is used to classify attacks that target many security services at the same time. As a result, the new classification methodology divides attacks into two groups: those that harm wireless communication technology and those that damage wired communication technology. Second, attacks are divided into one of five categories in each wireless communication technology, (Kordy et al., 2011).

3.2.1.2.1. Fabrication:

This classification comprises attacks aimed at impersonating trustworthy entities in IOT infrastructure in order to obtain access to certain privileges and commit criminal acts. For example, in a wireless IOT network, an attacker spoofs a master entity and instructs slave entities to change their functions.

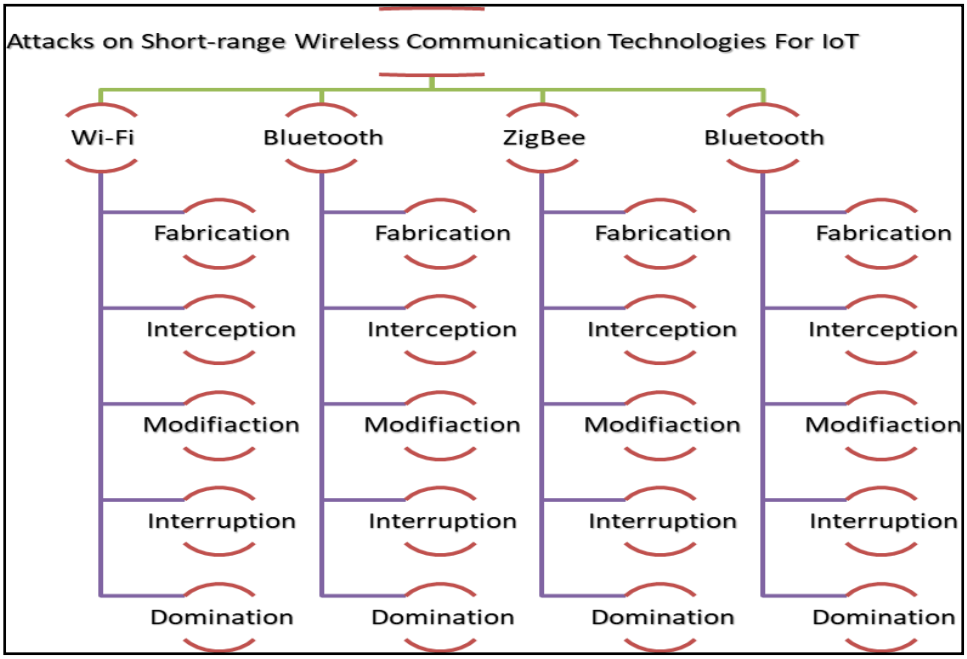

Figure (3) Schem of wireless IOT attack classification including ZigBee, WiFi, RFID showed modification, interruption and domination

3.2.1.2.2. Interception:

This classification includes all forms of assaults aimed at jeopardizing the security of IOT wireless systems. An attacker (called an eavesdropper in this scenario) catches wireless communications over the air and analyses it to extract secret and private information.

3.2.1.2.3. Modification:

This type includes all types of attacks that try to tamper with the content of messages and data stored in a wireless IOT system and its infrastructure including intercepting network communications, changing their contents, and resending the messages to IOT nodes that hadn't yet received them.

3.2.1.2.4. Interruption:

This type includes attacks aimed at denying legitimate users access to a set of services supplied by an IOT infrastructure so the attacker could disable a set of nodes in a wireless IOT network.

3.2.1.2.5. Domination:

This class's attack can be used as a prerequisite for other classes' assaults where the attacker can shut down the network or prevent specific clients from connecting by knowing the network password and impersonating the network access point moreover this class includes assaults aimed at simultaneously compromising numerous security services.

3.2.1.3. Create IOT risks Data Base:

When compared to traditional enterprise systems, IOT databases have a very different set of requirements. NOSQL is a partitioned, scale-out database with in-memory storage and processing for high performance and scalability. It provides a versatile key-container data paradigm that can be easily used to work with a wide range of data types. It uses cloud computing and includes numerous frameworks such as databases and data processing. Edge Computing, Gateway Aggregation, and Direct Connectivity are the three main components of an IOT system. The edge gateway, the edge device, and the actual edge sensor are the three sorts of devices. That information can be disseminated using NOSQL's native APIs or another messaging system. A gateway device can connect to a NOSQL cluster using native APIs or send data to the datacenter using a secondary communications protocol. For controlling their nodes, distributed systems like NOSQL systems often use either a Master-Slave design or a Peer-to-Peer architecture. The key-container model of data in NOSQL makes it simple to use many forms of data. The containers can utilize any key or a timestamp to make temporal data processing easier. NOSQL contains built-in aggregate and geometry functions, which let developers to quickly create queries without having to write their own sophisticated methods, (Nasar, and Abu Kausar, 2019).

3.2.2. Phase (2): IOT scanning Risks (intrusion Risks Detections):

When used as a bridge between low power IPv6 networks and normal IPv6 networks, a wireless sensor network consists of a number of sensor nodes called motes. The sensor nodes in a Wireless Sensor Network (WSN) communicate with each other and collaborate when routing data sent to a dedicated node often called the sink node, which is known as the "base station" or "border router. The sink node's job is to handle all of the incoming and outgoing communication to and from the Wireless Sensor Networks. Contiki is a real-time operating system for sensor nodes with IPv4 and IPv6 protocol stack compatibility, as well as more contemporary protocols like 6LoWPAN (IPv6 over Low Power Wireless Personal Area Networks) and RPL (Routing Protocol for Low power and Lossy Networks). Contiki's sensors are either synchronous or asynchronous. "Protothreads" are a significant element of the Contiki. Threads that don't have a dedicated stack in memory are called protothreads and they're incredibly very efficient. The protothreads are used to provide a flow in Contiki programs, and they are driven by events, (Dunkels, et al., 2014).

3.2.2.1. Basics about Intrusion Detection:

Contiki's sensors are synchronous and can be used with an intrusion detection system (IDS) which divided into four categories and used to identify attacks and notify them to a system for prevention of an attacker. The four types of IDS are; Signature-based IDS, anomaly-based IDS, specification-based IDS, and hybrid-based IDS which are based on detecting "known attacks" by looking at parameters that are known to indicate a specific attack. This approach has a low false positive rate, but it can't detect assaults that aren't already known to the system (Kumar et al., 2016). The detection approach is designed to detect common IOT assaults. It is based on the energy consumption of the node's radio communication hardware as a result of any sort of assault that aims to deplete a node's resources by flooding the node's radio communication. The technique reads the node's energy usage and stores values on how it changes over time in a suitable data structure. In order to detect assaults, an algorithm analyses the collected data (Kumar et al., 2016). The linear regression algorithm is known as LiReg as reported by, (Johan & Vester, 2017). The algorithm determines the difference between the current and expected energy values. The difference is then multiplied by the average energy consumption value for the collected data to get the difference in comparison to the average consumption value. Due to the difference in compared to the average value, the abrupt rises in energy consumption that are out of the ordinary in relation to the node's history. The decision to compare the difference to the average was made as part of the design process. If the percentage produced by dividing the difference with the average value exceeds a specific threshold, the node is considered to be vulnerable to an IOT attack, (Johan & Vester, 2017).

3.2.3. Phase (3): IOT Risks Matching:

The phase (3) showed model for matching between IOT Risks catching in phase (2) and IOT Risks registered in IOT Risks Data Base. If matching process found the IOT Risks Name and ID It continuous to Phase (4), if not it going to update IOT Risks DataBase by the name and Id of new IOT Risks founded.

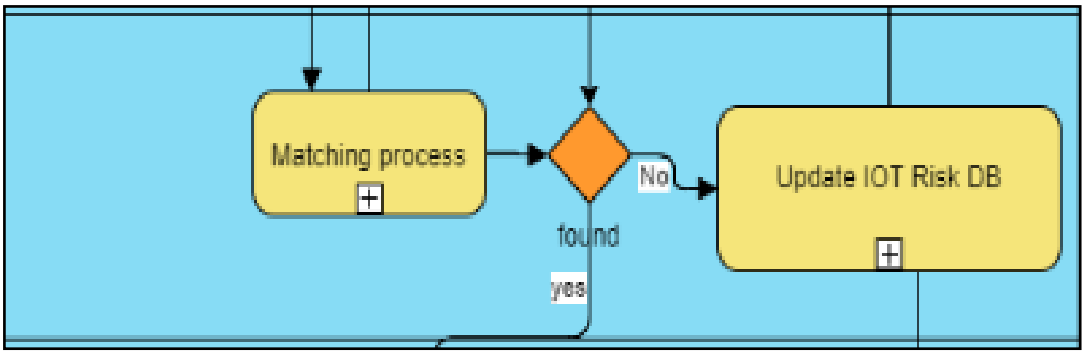

Figure (4) IOT Risks Matching process.

3.2.4. Phase4: IOT Risks Prediction Report:

This phase demonstrates results of IOT Risks matching in phase (3) according IOT Risks Classification in Phase (2).

3.2.5. Interruption attacks: (Kordy et al., 2011)

3.2.5.1. Interruption on Wi-Fi:

Wi-Fi is completely vulnerable to network availability attacks; all attacks on Wi-Fi availability are the result of a Wi-Fi authentication implementation that is only partially implemented. IoT risk-defense tree based on interruption attacks on a Wi-Fi IoT system are illusterated in figure (5).

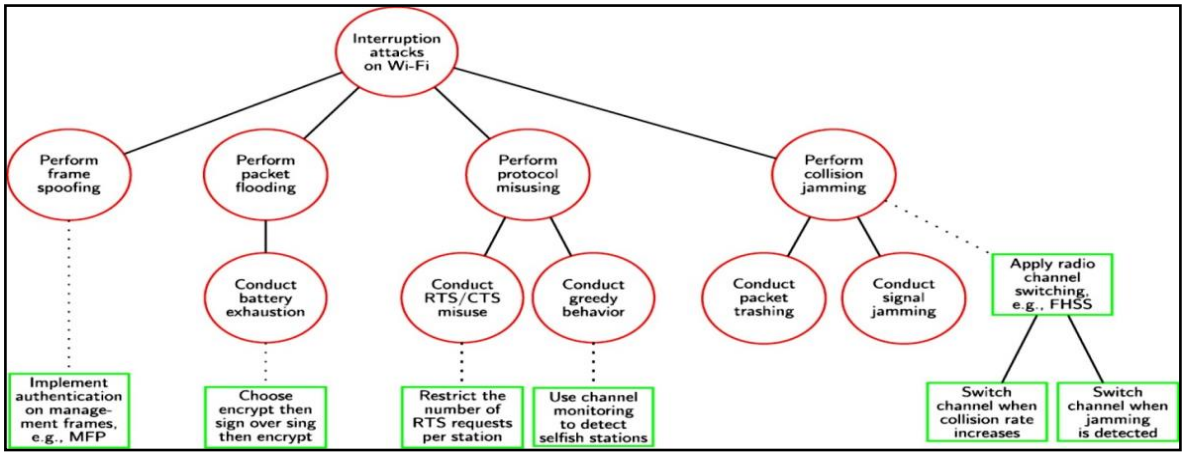

Figure (5) show tree of An IOT Risks-defense based on interruption attacks on a Wi-Fi IOT infrastructure (red: attacks,: green: defenses)

3.2. 5. 2. Domination attacks on Wi-Fi:

Multiple security services have been compromised as a result of these Wi-Fi hacks. An IOT risk-defense tree based on domination attacks on a Wi-Fi IOT infrastructure as shown in figure (6).

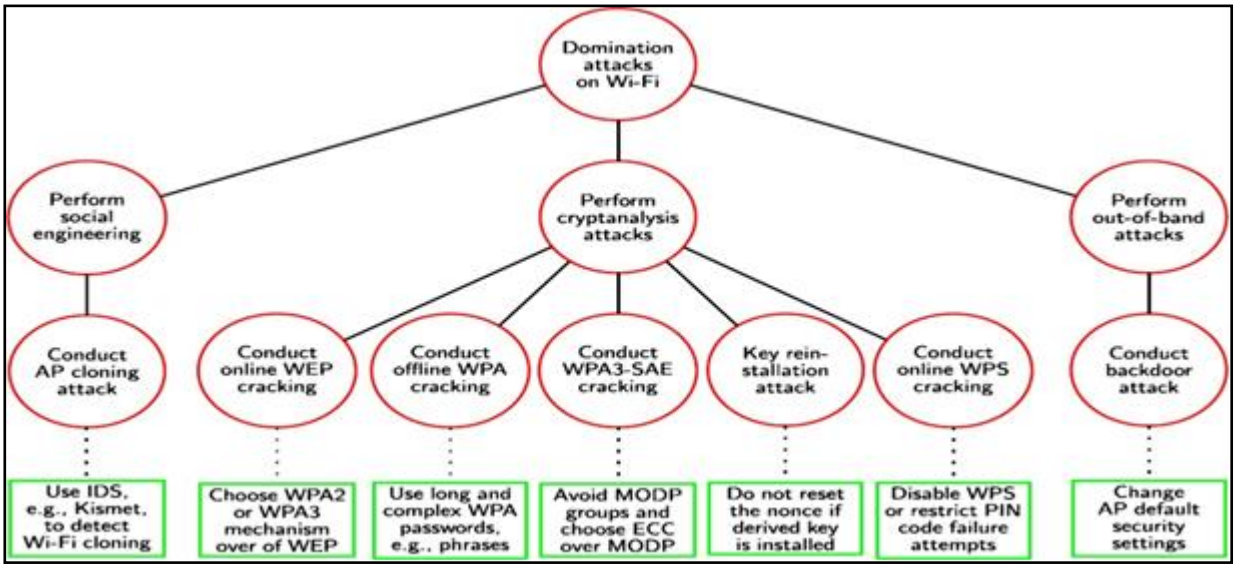

Figure (6) Tree of An IOT Risks-defense tree depend on domination attacks on a Wi-Fi IOT infrastructure (red; attacks,: Green: defenses)

3.2.5. 3. Fabrication attacks on Bluetooth:

These attacks allow attacker to mimic a genuine Bluetooth user in order to get access to particular privileges and inflict network harm. IOT risk-defense tree based on fabrication assaults on a Bluetooth IOT system are illustrated in figure (7).

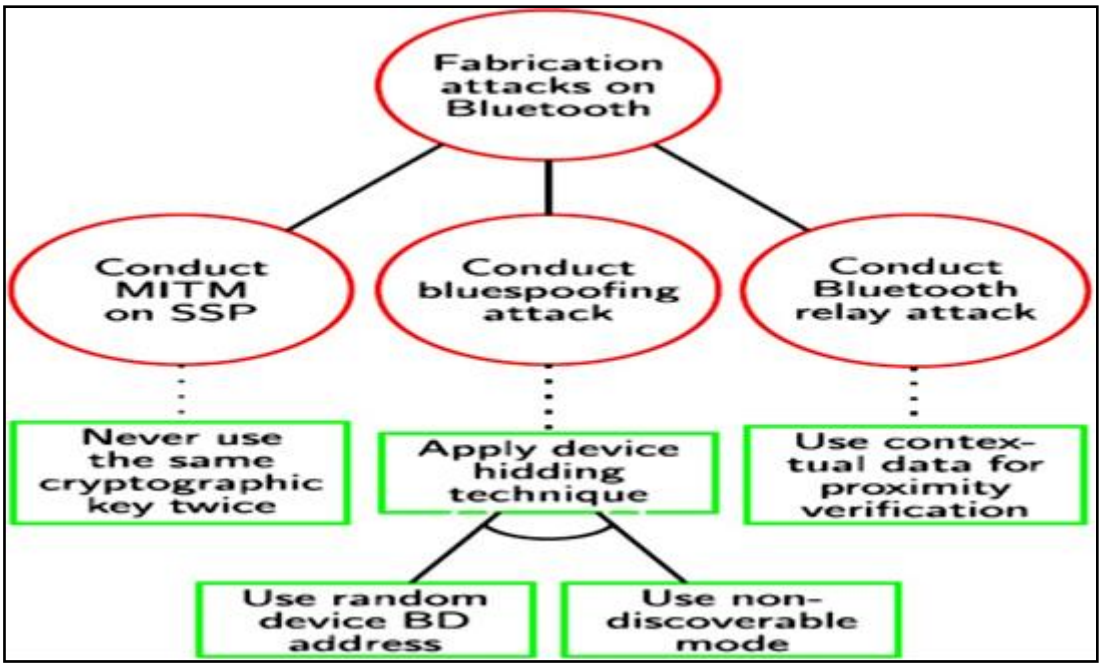

Figure (7) Tree of An IOT Risks- defense depend on fabrication attacks on a Bluetooth IOT infrastructure (red: attacks,: green defenses)

3.2.5.4. Domination attacks on Bluetooth:

These vulnerabilities allow an attacker to pose as a genuine Bluetooth user in order to get access to particular privileges and inflict network harm. The risk-defense tree for IOT depend on fabrication attacks on a Bluetooth IOT system (8).

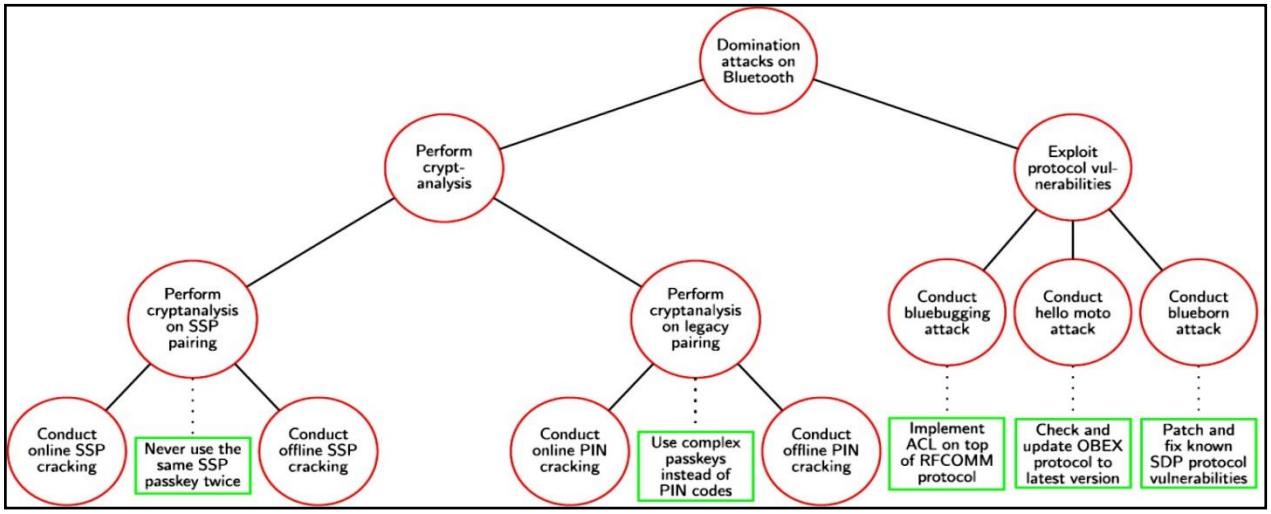

Figure (8) Tree of IOT Risks- defense based on domination attacks on a Bluetooth IOT infrastructure (Red: attacks,: Green defenses)

3.2.5.5. Fabrication attacks on ZigBee:

There are a variety of attacks aimed at getting over ZigBee's authentication systems, such as the IOT Risks-defense tree based on fabrication assaults on a ZigBee IOT infrastructure illustrated in figure (9).

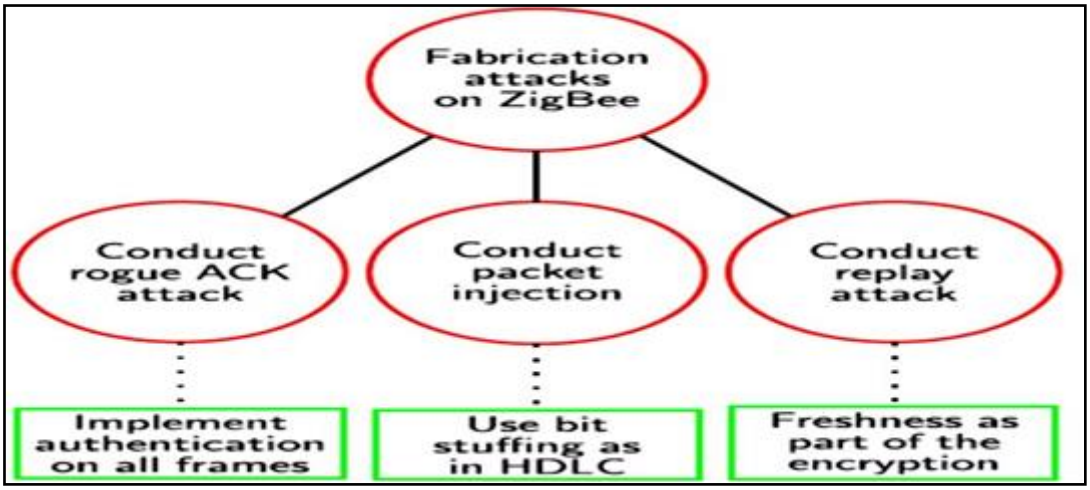

Figure (9) Tree of An IOT Risks-defense based on fabrication attacks on a ZigBee IOT infrastructure (Red: attacks,: Green defenses)

3.2.5.6. Interruption attacks on ZigBee:

There are a variety of attacks aimed at making a ZigBee network according to the IOT Risks-defense tree based on interruption attacks on ZigBee IoT infrastructure. illustrated on figure (10).

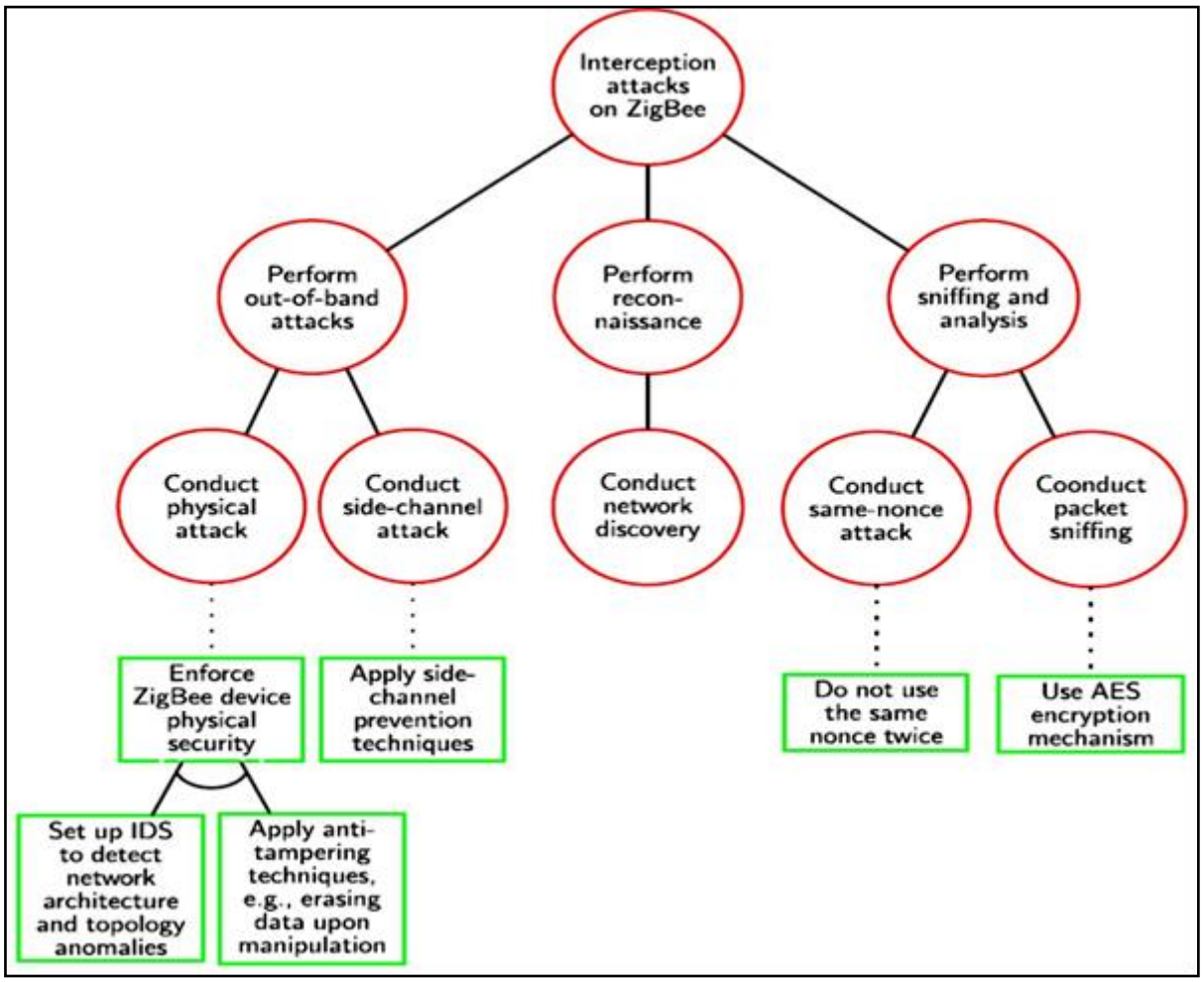

Figure (10) Tree of IOT Risks-defense defense tree based on interception attacks on a ZigBee IOT infrastructure (Red: attacks,: Green defenses)

3.2.5.7. Interruption and Fabrication attacks on RFID:

Fabrication attacks on RFID IoT infrastructure enables an attacker to spoof an RFID tag and defeat RFID-based authentication systems such as keyless access systems and contactless authentication systems, according to the IOT Risks-defense tree as illustrated on figure (11) and figure (12).

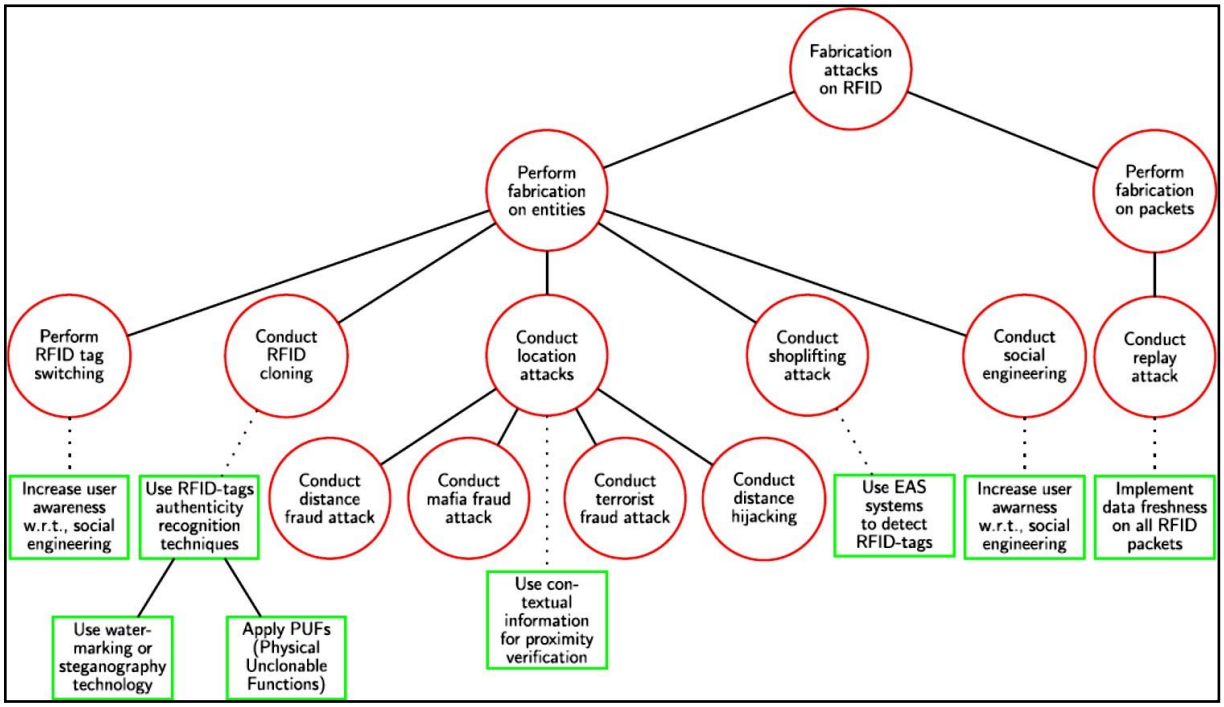

Figure (11) Tree of IOT Risks-defense tree based on interruption attacks on a ZigBee IOT infrastructure (Red: attacks, Green defenses)

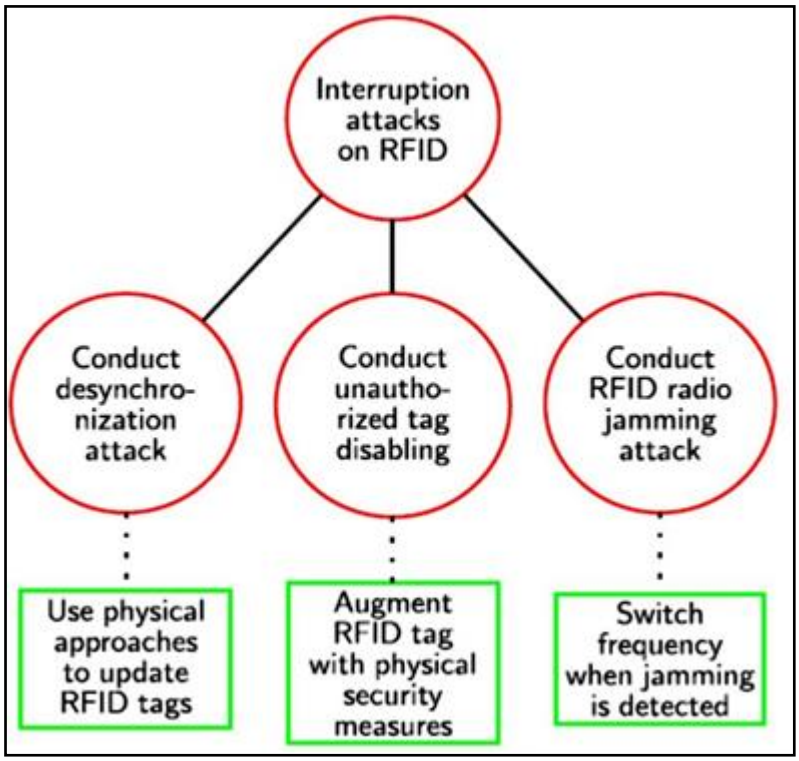

Figure (12) Tree of IOT Risks-defense based on fabrication attacks on RFID IOT infrastructure (Red: attacks,: Green defenses)

4. Results Finding and Discussion:

4.1. Data extraction and analysis:

The data extraction in this study depend on secondary data from previous studies including Traditional detection security and privacy hazards methodologies used the security risk in the proposed IOT model for the IOT risk-based strategy that published on academic sites; Google scholar, Pub Med, research Gate in order to an overview of threat models in the IOT. Also depends on primary data from survey for some experts where each expert was given a brief background on the research's goal before being asked interview questions.

4.2. Findings and discussion:

The necessity for contemporary models that are more flexible than previous approaches has been highlighted numerous times in recent years, particularly since the introduction of IOT. The IOT risk-based strategy offers a flexible approach to determining access. The access decision is made using the IOT risks database connected with the access request as a factor. Through conversations with IOT security domain experts, the suggested model has been developed and validated. The goal of the expert interviews was to validate the model and the researcher's implementation plan. Each expert was given a brief background on the research's goal before being asked interview questions. The first question concerned their thoughts on the suggested model in general. The model has piqued the curiosity of most specialists when the researcher initially revealed it to them. They verified that it will be beneficial to the IOT business and advised contacting interested companies in order to obtain further funding to complete the research. The second question was the model methodologies used the security risk in the proposed IOT model. The model was then tested with the following question. In terms of model context, the majority of experts felt that the proposed model is appropriate for applicants in IOT applications, as it allows for the use of real-time contextual data to make access decisions and can be used with a range of IOT applications such as model context which impact on decisions to be made based on real-time information. They also stated that the device is compatible with a variety of IOT applications. They suggested starting with a single IOT application and attempting to detect additional risk factors associated with this specific IOT Model in addition to the currently mentioned risk factors. The experts were questioned about the importance of rating IOT risk variables in order to determine the final report of the proposed Model. The majority of experts agreed that all of the risk factors included in the suggested model are critical. Interception, interruption, dominance, and dominance are the most effective elements, followed by action severity and user context. According to some experts, risk factor rankings may need to be adjusted depending on the application domain. Following that, experts were quizzed on the best risk assessment approaches to use in the present model and how to assess the security risk associated with each access request. The majority of

experts agreed that determining the best risk estimation technique is the most important and difficult part of putting the model into practice. Risk assessment attempts to forecast the future in terms of the likelihood of a specific incident occurring and its consequences; evaluating the risk without a dataset outlining the effects of various access control scenarios would make assessing the risk more challenging. Experts recommended that existing IOT risk-based models be reviewed for different risk estimation methodologies. In this thesis, the researcher looked at various risk estimation methods. Many experts also proposed employing a fuzzy logic technique. Some experts advised that one of the machine learning techniques be used to determine the model's security threats. They recommended picking a specific IOT application, finding a related dataset, and using an ANN to achieve high performance with a mitigation plan against various attacks and malicious actions during the access session while taking into account the response time to detect and prevent the attack or malicious action. Some experts, on the other hand, advocated splitting the grant band into two groups: one without monitoring for users with very low security risk values, and another with monitoring for users with security risk values less than the threshold risk value. Finally, experts were asked if a proposed Model for Predicting IOT Risks was adequate to protect IOT Users. The proposed model, which can provide IOT users with prevention by knowing IOT risks, is generally recommended by experts. The proposed model was reviewed by IOT security specialists. Most experts believe that the proposed paradigm is intriguing and will serve as a good starting point for increasing information sharing and availability in IOT applications while also addressing security concerns. Twenty IOT security experts confirmed the researcher's methodology and suggested fresh information about risk estimation approaches and risk factors, validating and refining the proposed model. A fuzzy logic technique will be utilized to quantify the security risk associated with access requests, as recommended by experts. The fuzzy logic will provide a flexible framework. Regarding risk factors, the proposed risks factors are appropriate as they can be adjusted to different IOT industry without need to change other factors. Furthermore, we investigate if the suggested model should be evaluated, as recommended by experts, and whether it can be used to forecast IOT security and privacy threats.

5. Conclusion

Traditional detection security and privacy hazards methodologies, which are static and context insensitive, cannot meet IOT security requirements due to the dynamic nature of the IOT. As a result, the goal of this study was to create a dynamic and adaptive suggested model that can adapt to changing IOT settings where IOT Risk-based Model is one of the dynamic models that estimates the IOT security and privacy risk linked with the IOT Risks Database using real-time contextual information. The present Internet of Things (IOT) model has been presented. Predict IOT Risks is the first of four steps in this methodology. Phase 1 involves manipulating IOT Risks. IOT Risks attacks are classified in the data base. This classification assigns a value to an attack depending on the security service that was compromised.

The classification used to examine assaults on Wi-Fi, Bluetooth, ZigBee, and RFID wireless communication technologies over the previous two decades. Phases (2) and phase (3) deal with detecting IOT dangers, whereas phases (4) and phase (5) manage the matching process between IOT outcomes and IOT Risks and Data Base. In the final phase, modify the prediction report. Twenty IOT security specialists were questioned to validate the proposed model and obtain additional information from highly experienced experts. The idea piqued the interest of most experts, who agreed that it would be beneficial to the industry. They recommended adopting fuzzy logic to undertake the IOT risk estimation method, especially if adequate datasets were not available. They also suggested focusing on a specific IOT application and identifying risk factors associated with it. They also suggested that a mitigation strategy be implemented to detect and prevent harmful acts in the monitoring and detecting process, and that the proposed model is appropriate and can be used to implement the proposed model. The presented model can be used to anticipate IOT security and privacy issues using a fuzzy logic approach in future research.

6. References

[1] A Comprehensive Analysis on the Security Threats and their Countermeasures of IOT2017International Journal of Advanced Computer Science and Applications (IJACSA)489-501

[2] A Critical Analysis on the Security Concerns of Internet of Things (IOT)2015International Journal of Computer Applications1-6

[3] A secure industrial Internet of Things (IIOT) framework for resource management in smart manufacturing2020IEEE117354-117364

[4] A Study of Key Technologies for IOT and associated Security Challenges2017The International Symposium on Wireless Systems and Networks (ISWSN)1-6, 19-22Lahore, Pakistan

[5] A Survey on the Internet of Things Security2013International Conference on Computational Intelligence and Security (CIS)663-667Leshan, China

[6] Authentication Protocols for Internet of Things: A Comprehensive Survey2017Protocols for Internet of Things: A Comprehensive Survey", Wiley 1-41

[7] Contiki-a lightweight and flexible operating system for tiny networked sensors200429th Annual IEEE International Conference on. IEEE, 2004455–462Local Computer Networks

[8] Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks2015Journal of Cyber Security65-88

[9] Denial of Service Attack Techniques: Analysis, Implementation and Comparison2006Systemics, Cybernetics and Informatics66-71

[10] Foundations of attack_defense trees," in Formal Aspects of Security and Trust2011Cham80-95Switzerland

[11] Huawei2018Tap Into New Growth with Intelligent Connectivityhttps://www.huawei.com/minisite/gci/assets/files/gci_2018_whitepaper_en.pdf?v=20180716.

[12] Improving Smart Home Concept with the Internet of Things Concept Using RaspberryPi and NodeMCU2018Proc. the IOP Conference Series: Materials Science and Engineering1-10

[13] Internet of Things (IOT): A vision, Architectural Elements, and Future Directions2013Elsevier, Future Generation Computer Systems1645–1660

[14] Internet of Things Security2017International Conference on Wireless Technologies, Embedded and Intelligent Systems (WITS)19-20Morocco

[15] Internet of Things Security: Layered Classification of Attacks and Possible Countermeasures2016Electronic Journal of Information Technology24-37

[16] Internet of Things: Architectures, Protocols, and Applications2017Journal of Electrical and Computer Engineering1-25

[17] Internet Refrigerator–A Typical Internet of Things (IOT)2015the 3rd International Conference on Advances in Engineering Sciences & Applied Mathematics (ICAESAM'2015)59-63, 23-24London (UK)

[18] 2017Intrusion detection system framework for Internet of Things M., S thesis

[19] IOT Security: A Layered Approach for Attacks & Defenses2017the International Conference on Communication Technologies (ComTech)104-110, 19-21 Rawalpindi, Pakistan

[20] IP Spoofing Attack Detection using Route Based Information2012International Journal of Advanced Research in Computer Engineering & Technology285-288

[21] Security in Internet of Things: Challenges, Solutions and Future Directions2016 the System Sciences (HICSS), 49th Hawaii International Conference on System Sciences5771- 5780Koloa, HI, USA

[22] Security in the Internet of Things: A Review2012International Conference on Computer Science and Electronics Engineering (ICCSEE) 648- 651, 23- 25Hangzhou, China

[23] 2017Security Management for the Internet of Things A Thesis of Applied Science at the University of Windsor University of Windsor Scholarship at UWindsor Electronic Theses and Dissertations, https://scholar.uwindsor.ca/cgi/viewcontent.cgi?article=6934&context=etd.

[24] Suitability of influxdb database for IOT applications2019 International Journal of Innovative Technology and Exploring Engineering1850-1857

[25] The Google Car: Driving Toward A Better Future?2014Journal of Business Case Studies7-14

[26] The Internet of Things: A Survey2010 Elsevier, Computer Networks2787–2805

[27] Threat-based Security Analysis for the Internet of Things2014Proc. the 2014 International Workshop on Secure Internet of Things, wroclaw35-43Poland