JOURNAL OF CRITICAL REVIEWS

ISSN- 2394-5125 VOL 09, ISSUE 01, 2022

Investigating The Role of The Internet Of Things (Iot) in The Growth of New Technologies in Society

Author: Faqeed Ahmad Sahnosh
Assistant Professor Department of Information Systems Faculty of Computer Science
Kabul Education University

Abstract

The idea of connecting devices and objects globally emerged with the advent of Radio Frequency Identification(RFID) technology. The concept then spread to the present perspective that in the near future, we will encounter a large set of heterogeneous objects that interact with each other in the physical world. Today, with the development of small networks, many similar devices have the ability to communicate with each other, which we call the "Internet of Things". Intranet of Things means the internal communication between members of different small networks, however due to incompatibility, these networks are not able to communicate with each other. Therefore, the creation of a single standard and protocol among the leading companies in establishing the compatibility of these communications, has led to the formation of a single global network called the Internet of Things (IoT). From the point of view of the Internet of Things, all real objects in the environment will have identities and will exchange communications in an integrated environment. The Internet of Things means the ability of all objects to communicate with each other and with humans, while identifying and discovering them under a single network. It is natural that creating such a network carries many risks. The World Wide Web, which has been popular for years, still has many security vulnerabilities that endanger property and even human lives. Under such circumstances, establishing security in a global network of objects, each with its own characteristics and limitations, relating to each other and to humans, would naturally be much more complex. The new conditions of the environment and the various features of the devices cause the Internet security of things to be given special attention and various architectures to be provided for it. Internet of Things security is a key issue in the implementation of this technology and extensive research is needed to protect the security and privacy of individuals in this regard. Lack of sufficient specialized knowledge is currently an obstacle for researchers to clarify the scope of the IoT in a methodical way. This study will address the literature and architecture of the Internet of Things, related tools, technology and their methods and functions to facilitate the needs of developers and improve comprehension directly or indirectly.

In this article, after introducing the Internet of Things and its advantages and applications, security in the Internet of Things is considered as a key axis and the requirements, challenges and proposed solutions for it are discussed.

Keywords: Internet of Things (IoT), Security, Latest Technologies, Society

Introduction

Today, more than two billion people worldwide use the Internet to use web pages, send and receive electronic emails, multimedia content and services, computer games, social networking programs, and other services. As more and more people gain access to the above information and communication infrastructure, more progress is being made, and the use of the Internet to communicate, exchange, calculate, and coordinate between machines and smart objects is evolving. It is expected that with these new applications around us, content and services will always be available. This new content will also be the keystone and way to develop new applications and new ways of interacting, entertainment and new ways of life. The Internet of Things, is a system of interconnected devices and networks, proposed by Kevin Ashton in 1991. This can be considered an innovation and revolution in the world of technology because it has updated the existing Internet base to an advanced high-level computing network, so that all the physical objects around us will be interconnected and uniquely identifiable. With this technology,

ISSN- 2394-5125 VOL 09, ISSUE 01, 2022

every object around us, such as mobile phones, cars, watches and accessories, will collect useful user data using different technologies, and this data which is collected from the environment are set to be used to perform various operations automatically.

As is known, the benefits of using the Internet of Things are obvious in all structures of human life. Here is some important IoT applications thematically that include the following [1].

Aerospace and aviation industry, automotive industry, telecommunications industry, medicine and treatment industry, independent living, pharmaceutical industry, food stores and supply chain management, manufacturing industry, oil and gas industry, environmental monitoring, transportation industry Land and sea, agriculture and reproduction, media and entertainment industry, insurance industry, recycling network, smart electricity grid, mining and mineral extraction, smart home, monitoring secret exams and elections, social and personal areas, social networks Intelligent, finding lost or stolen objects, etc., which are described as follow.

Smart Cities: The smart city greatly mechanizes the infrastructure of public services and business activities by creating a communication network. Sensors are distributed throughout the city to collect information on human behavior in terms of consumption, use of facilities, and other areas related to social behavior. Upon receiving this information, the city supervisory bodies will take the necessary measures to increase the living standards of the people living in the city.

Transportation industry: With the advent of the Internet of Things, this industry will undergo many changes, however, there are still limitations to reach that level of communication between objects in the transportation industry. For example, instant access to traffic information is not yet possible. By solving this type of problem and replacing the old transport vehicles with devices connected to the Internet, also prevents the occurrence of many accidents. Google is currently building a new car that can travel up to 1,000 miles without human help and up to 14,000 miles with little human help.

Aviation: In the aviation sector, the Internet of Things(IoT), can use sensors to measure, monitor, and continuously monitor aircraft pressure, heat, and vibration. This feature provides instant access to aircraft information and passenger conditions for both the care unit and the pilot. RFID tags attached to aircraft components can prevent the use of counterfeit components in aircraft [13].

Energy: In the energy sector, the IoT can help monitor and manage energy consumption. Smart applications make it possible to provide better services to consumers in addition to effective performance in energy conservation. Smart connectors regulate their consumption by sending signals to consumers. Furthermore, to reduce consumption costs during peak hours, this also prevents interruptions due to increased load. Sensors installed in sensitive areas of gas transmission pipes can measure the pressure and volume of gas transmitted at any time and in Authorize supervisors of the energy transfer process to take the necessary action in an emergency before an accident occurs.

Production Cycle Management: Many manufacturing companies use RFID tags to monitor and manage their products. In addition to making cataloging easier, these tags also prevent counterfeiting. The sensors connected to the products can inform the consumer about the accuracy and health of the device. Monitoring the commercial items from production until it reaches the consumer is the biggest gift the IoT will bring to manufacturing companies. We must say that the Internet of Things will break the way of communication that is common today and the focus is on human data. Technologies such as Fi-Wi, RFID, instant location, and sensor networking will allow us to manage nature and objects in the future.

In fact, the Internet of Things is a concept in which small microprocessors are the interface of intelligent objects with sensors, communication drivers that are equipped with energy sources and can perform multiple processes and communicate with each other, which is described in Figure 1. And the parts of an Internet of Things device are marked with data. As we can see, IoT technology combines different communication methods such as RFID, 5G / 4G / 3G, Wi-Fi, ZigBee, compact devices and sensors, and in applications such as environmental monitoring, weather forecasting, transportation, trade, Used in medicine, military applications, and other applications.

ISSN- 2394-5125 VOL 09, ISSUE 01, 2022

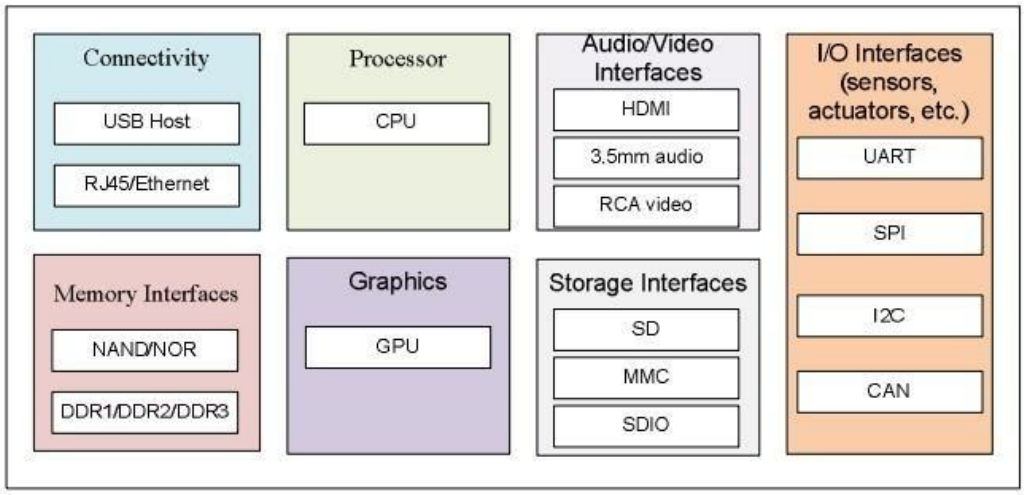

Figure 1: Parts of an Internet of Things device

Along with IoT, the use of a powerful processing core such as the "cloud" is clearly defined, and the combination of wireless sensor networks with cloud computing makes it possible to share and analyze sensor information instantly. The issue of storage capacity may also be addressed by low-cost cloud computing methods, which are widely used in distributed and mobile environments to provide security and easy access to information. Areas of application of cloud platforms for the Internet of Things such as equipment management, data management, and monitoring management, etc. are clearly shown in Figure 2.

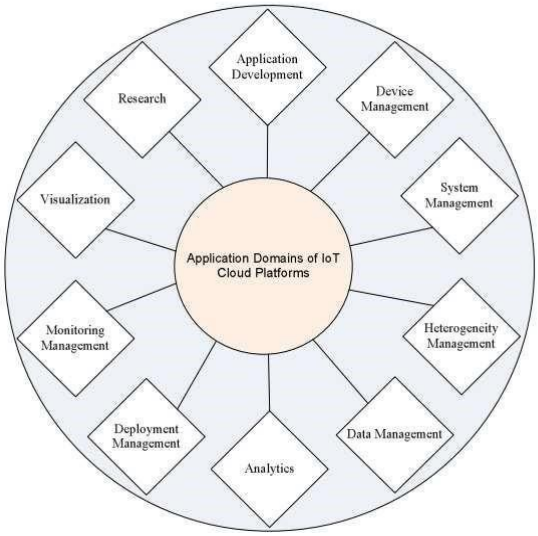

Figure 2: Areas of application of cloud platforms for the Internet of Things

Extensive research on the Internet of Things is underway, and the issue of IoT will soon become a reality. According to GARTNET theory, it is expected that by 2022 more than 30 billion identifiable objects will be part of this computing network.[3] however, when there are interconnected devices in this large network, new security and privacy issues and theories will emerge. Will and all connected devices will be at high risk of hackers because hackers are waiting for security gaps to force the devices to do whatever they want. The Internet of Things has great flexibility and usability, but it also has the potential to break

ISSN- 2394-5125 VOL 09, ISSUE 01, 2022

security. There is also a lot of discussion about agreement on this issue, but these discussions seem to have no future without successfully resolving the security threats. Due to their easy access to objects, they can easily be used by hackers at any time. It does not matter how companies think about the security of their products, because they are always witnessing all kinds of attacks. Because these devices are connected to users' daily lives, security should be a top priority. There must be a number of security infrastructures to limit and resist IoT security threats. The second section describes the overall structure of the IoT, the third section describes the security objectives, and the fourth section describes the important security challenges and the subject of each layer. Section 5 examines the IoT security architecture and secure architecture proposed by leading companies in this field. The sixth section is the conclusion and presentation of the proposal in the field of IoT.

IoT Standards

According to the Internet of Things ecosystem, different standards are required in different areas such as wireless communication, technical, application, and service quality, and therefore different organizations and institutions are involved in its standardization. The following are the standards and protocols in the Internet of Things ecosystem, and some of the companies operating in these areas are discussed in detail below.

Table 1: Standards and protocols in the Internet of Things ecosystem

Area	Standard
Security	*TCG, Oath 2.0, SMACK, SASL, ISASecure, ace, CoAP, DTLS, Dice*
Management	*IEEE 1905, IEEE 1451, …*
Software	*Mbed, Homekit, AllSeen, IoTvity, ThingWorks, EVRYTHNG, …*
Operating System	*Linux, Android, Contiki-OS, TinyOS, …*
Hardware	*ARM, Arduino, Raspberry Pi, ARC-EM4, Mote, Smart Dust, Tmote Sky, …*

Other standards and protocols are also set out in the IoT Network and IoT technologies that are used. The IoT plans to combine different telecommunications technologies to create a new service. A clear example is the combination of GPS, WLAN, Bluetooth Power Low, NFC, GSM, and WSNs with SIM card technology. In this technology, the smart device will be part of the mobile phone, and the information through the SIM card between other NFCs will allow simple and secure communication between objects that are close to each other [51]. Therefore, by combining this technology and the possibilities of a SIM card, the collection of objects in the workplace or at home can be easily planned and managed by a mobile phone.

The IEEE has introduced a variety of standards, including 802.11. The foundation of many of the equipment and facilities available to us today, such as WiMax, USB, Ethernet, Wi-Fi, was established by the IEEE, which is compared in the table below to match existing communication technologies in terms of standard, operating frequency, transmission rate, cost, etc. Items have been reviewed.

Introduction to Zigbee Protocol and its Technology

ZigBee is an example of an intelligent network between reputable companies providing low-cost short-range services with a set of high-end communication protocols based on 802IEEE low-power digital transmitters and receivers for the network. Use personal wireless with low data rates. ZigBee was created to define a simpler and cheaper technology than Bluetooth for personal wireless networks. With the help of ZigBee, more than 64,000 devices can be connected wirelessly through the network.

Three types of devices can be found in ZigBee networks:

ISSN- 2394-5125 VOL 09, ISSUE 01, 2022

- Coordinator
- Routers
- Terminal devices

Coordinators monitor the layout and security of the network. Routers extend the network board, and terminal devices are responsible for specific sensory or control functions. However, most of these devices can have more than one function, for example, a device can act as a router for messages coming from other parts of the network while controlling the lighting equipment.

From the IoT perspective, all real and legal objects in the environment will have identities and will exchange communications in a single environment. The Internet of Things means the ability of all objects to communicate with one another and with humans while identifying and discovering them under an integrated network. Naturally, creating such a network carries many risks. The World Wide Web, which has been popular for years, still has many security vulnerabilities that endanger property and even human lives. Under such circumstances, establishing security in a global network of objects, each of which, with its characteristics and limitations, communicates with each other and with humans, will naturally be much more complex. The new conditions of the environment and the various features of the devices cause the Internet security of objects to be given special attention and various architectures to be provided for it.

Literature Review

In recent years, many research has been done on the Internet of Things and how to implement it, and the subject of IoT will soon become a reality in all matters of life. According to GARTNET theory, by 2022, more than 30 billion identifiable objects are expected to be part of this computing network. [3] However, when there are interconnected devices in this large network, security issues and theories and new privacy will be created and all interconnected devices will be exposed to a high risk of hackers because hackers are waiting for security gaps to force the devices to perform any operation they want. There are risks, but it also has the potential to break security. There is also a lot of large-scale debate over agreement on this issue, but these debates seem to have no future without a successful resolution of the security threats. [4] Due to their easy access to objects, they can easily be used by hackers at any time [5]. It does not matter how companies feel about the security of their products because they are always waiting for all kinds of attacks. Therefore, they must ensure that their security patches are available whenever and wherever they are needed. Because devices are connected to users' daily lives, security should be a top priority. There must be many security infrastructures to limit and resist threats, accessibility, and Internet security of things [6].

Today, with the formation of small networks, a large number of homogeneous devices can communicate with each other, which are known as "intranet objects". IoT means to communicate internally between members of different small networks, but due to incompatibility, these networks are not able to communicate with each other. Therefore, the creation of a single standard and protocol for the compatibility of these communications has led to the formation of a single global network called the Internet of Things.

In general, IoT has four important key levels, which are described below.

1. Receiving layer: The receiving layer includes different types of data sensors such as RFID, barcodes, and other network sensors. The main purpose of this layer is to identify unique objects and deal with data collected from the real world using relevant sensors.
2. Network layer: The purpose of this layer is to transfer the data collected from the receiving layer to any information analysis and processing system that the transmission operation is through communication networks such as the Internet, mobile phone network, or any type of reliable network.
3. Middle informed layer: This layer includes systems of analysis and information processing that undertake automatic operations based on the results of processed data and connects the system to

ISSN- 2394-5125 VOL 09, ISSUE 01, 2022

the database and stores the collected information. This is the server layer that guarantees the same types of services between interconnected devices.

4. Application layer: This layer recognizes different practical IoT applications based on the needs of users and different types of industries such as smart homes, smart environment, smart transportation, and smart hospital, etc. [11]

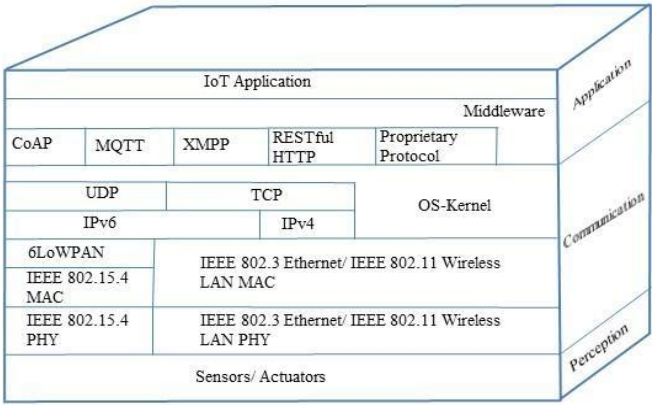

Figure 3. Protocols used in the Internet of Things

a) Data confidentiality

Data confidentiality means the ability to ensure that data is confidential to each user using a variety of methods that prevent the disclosure of data to unauthorized persons and the data can only be accessed by authorized users. Many security methods have used encryption methods to ensure the confidentiality of data, in which the information is encrypted, in which case it is difficult to access the data and use it and verify it in two steps by unauthorized persons. In this case, the authentication is created by two interrelated components, and access is allowed only bypassing both components of the authentication test. The most common type of authentication is biometric verification, which is uniquely identifiable. Internet-based devices from network sensor groups do not disclose their data to neighboring groups. Similarly, tags do not transmit their data to unauthorized readers [12].

b) Data comprehensiveness

Data comprehensiveness refers to the protection of useful data from cybercriminals in connection with some common tracking methods, so that data manipulation is accompanied by system restrictions [13]. Methods to ensure the accuracy and authenticity of data such as check checksum and cyclic redundancy, which are error detection methods for some data. Also, the ability to continuously synchronize data to backup and control the type of feature keeps a file record from changing in the system. It recovers the accidentally deleted file, thus ensuring data integrity. So when authorized users have access to data on IoT-based devices, ensure that they are in their original form.

c) Data availability

One of the main goals of IoT security is to make the required data available to its users when needed and at the moment. Data availability ensures that authorized users have normal access to their information resources under normal and abnormal conditions. Slowly, firewalls are required. Also, the availability of data prevents unfavorable conditions that prevent the flow of information. In the event of a system failure or various system conflicts, to ensure the availability of data, there are backup and redundancy methods that copy parts of the system.

ISSN- 2394-5125 VOL 09, ISSUE 01, 2022

d) Security challenges and theories

There have been many advances in the Internet of Things in recent years, yet there are still many security issues that need to be addressed. In this section, some of the threats that need special attention are discussed and evaluated.

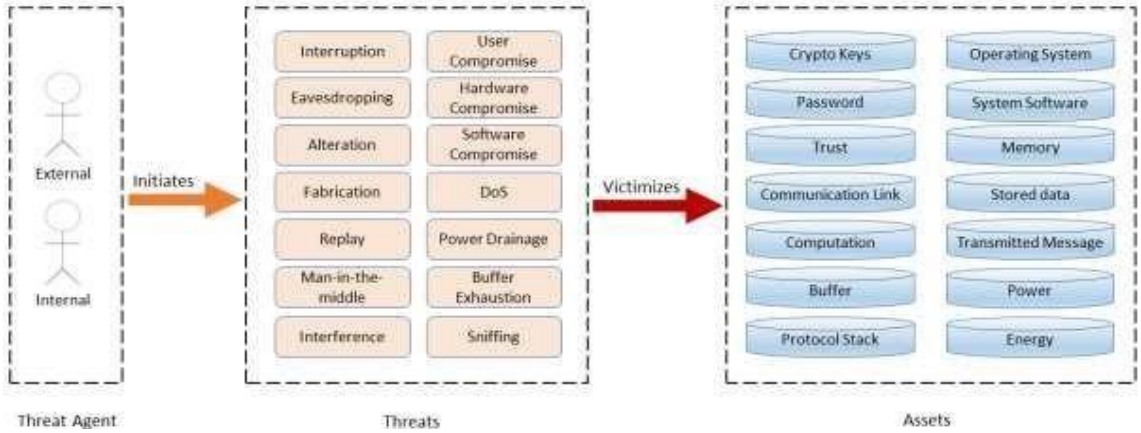

Table 2: Comparison of existing communication technologies

Parameters	WiFi	Wi MAX	LR-WPAN	Mobile Communication	Bluetooth	LoRa
Standard	IEEE 802. l l a/c/b/dlg/n	IEEE 802.16	IEEE 802.15.4 (ZigBee)	2G•GSM,CDM A 3G-UMTS, CDMA2000 4G-LTE	IEEE 802. I 5. 1	LoRaWAN R l .O
Frequency Band	5GHz-60GHz	2GHz-66GHz	8681915 MHz,2.4 GHz	865MHz, 2.4 GHz	2.4GHz	8681900MHz
Data Rate	IMb/s - 6.75Gb/s	J Mb/s - I Gb/s (Fixed) 50-100 Mbls(mobile)	40-250Kb/s	2G: 50-100 kb/s 3G:200 kb/s 4G:O. -I Gbls	l -24Mb/s	0.3-SOKb/s
Transmission Range	20-100m	<50Km	10-20m	Entire Cellular Area	8-10m	<30Km
Energy Consumption	High	Medium	Low	Medi um	BluetootkMediwn BLE: Very Low	Very Low
Cost	High	High	Low	Medi um	Low	High

The general classification for the IoT is as follows:

- M2M (M2M Devices of Internet): from various devices such as car sensors (for receiving various types of data) such as engine malfunction) by a network (mostly cellular wireless networks, sometimes wired and sometimes hybrid) connected to a central server, uses to turn the collected events into meaningful information.
- RFID (Objects of the Internet): Use of radio waves to transmit data to a reader for object identification and tracking purposes.
- WSN (Transducers of the Internet): Sensor networks include a set of autonomously distributed sensors that spatially monitor physical and environmental conditions such as temperature, pressure, motion, or pollution, and work together to transmit their data from within the network to

ISSN- 2394-5125 VOL 09, ISSUE 01, 2022

a Transfer to a central location. Most of these networks have a short-range wireless mesh structure and are sometimes wired or hybrid [32].

- SCADA (Controllers of the Internet) is an autonomous system based on closed-loop control theory or an intelligent system that monitors, connects, controls, and monitors equipment through a network (mostly wired with short-range and sometimes wireless or hybrid).

Application of IoT in Automotive Industry

Smart cars, trains, buses and even bicycles are being equipped with sensors with high processing power. Including IoT applications in the automotive industry can be used to use intelligent equipment to observe and report different parameters of tire pressure from estimating the distance from other vehicles moving on the road. Equipment connected to vehicle parts including information Such as the name of the manufacturer and the time and place of production, serial number, type of production code and the exact location of the part in each vehicle. In the field of Automotive industry (DSRCs) such as (V2V), (V2I) and technologies create intelligent transportation systems that result in Car and passenger safety and traffic management are all part of the IoT infrastructure. In the form of the next generation of communication between cars Are shown when IoT appears.

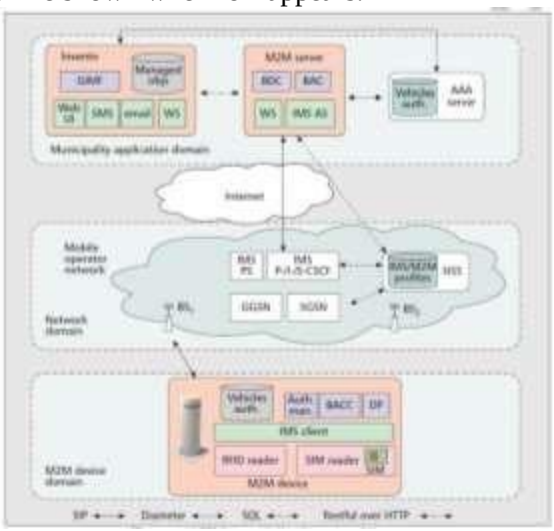

Figure 6. M2M based distributed architecture.

Above the sensors are the necessary facilities of a predicted network that can be local area networks (wired or wireless) or personal networks with small dimensions (cable or wireless, such as ZigBee, UMB, etc...). Sensor power consumption and data transfer rate is low, which is why we need a wireless sensor network or WSN (derived from a wireless network sensor) that after collecting the information, it can provide it to the destination for processing. Sensors based on application and group data types - such as peripheral sensors, military sensors, body sensors, home sensors, etc. (aggregation sensors, as are gateway units that can be connected to the network. Sensors that do not require a gateway connection can connect directly to the Internet via a WAN interface. At the lowest level we have tags that include RFID and barcode on it are sensors and actuators.

Here are some important, common, and related IoT-related standards and protocols (Figure 6) provided by these standardization centers:

SOAP[1]: A protocol for detecting the exchange of information in computer networks [28].

[1]Simple Object Access Protocol

ISSN- 2394-5125 VOL 09, ISSUE 01, 2022

IPV6[2]: It is an Internet layer protocol used to transmit data over multi-IP networks. LOWPAN36 is a special type of IPV6 protocol that complies with IEEE 4.15.802. The transfer rate in this protocol is 250 kbps [21].
UDP[3]: This protocol is used in IP networks with a user server.
DTLS[4]: This protocol allows server and client applications to communicate with each other in a way that prevents eavesdropping, tampering, or message forgery.
MQTT[5]: This protocol allows the transmission of messages in a very light way; Which is very useful for communicating with distant places.
COAP[6]: This protocol is designed to use in the application layer. In this protocol, specialized requirements such as multi-part support and simplicity are observed.
SMCP[7]: This protocol is based on the COAP protocol and is very suitable for embedding in equipment.
XMPP[8]: This protocol is suitable for transmitting a wide range of applications including instant messaging, chat and voice and video calls.
Below we have organized all the objects of the Internet of Things in existing architectural models similar to the OSI model and the internal protocols of the lower layers for the Internet of Things [8.]

1. *Infrastructure (ex: 6LowPAN, IPv4/IPv6, RPL)*
2. *Identification (ex: EPC, uCode, IPv6, URIs)*
3. *Comms / Transport (ex: Wifi, Bluetooth, LPWAN)*
4. *Discovery (ex: Physical Web, mDNS, DNS-SD)*
5. *Data Protocols (ex: MQTT, CoAP, AMQP, Websocket, Node)*
6. *Device Management (ex: TR-069, OMA-DM)*
7. *Semantic (ex: JSON-LD, Web Thing Model)*
8. *Multi-layer Frameworks (ex: Alljoyn, IoTivity, Weave, Homekit)*
9. *Security*
10. *Industry Vertical (Connected Home, Industrial, etc)*

Security Challenges and Theories

as already noted, IoT has many achievements in our daily lives, however, there are still many security challenges that need to be addressed. This section discusses some of the threats that need special attention.
There are five major concerns about IoT security:

First concern:
In the process of designing smart products, so much attention has been paid to security as to the application. Some manufacturers do not consult with any security expert in the manufacture of their product and the result is an intelligent device that is vulnerable to the intrusion of attackers.
solution:
Before preparing any smart device, even the simplest ones, make sure that the manufacturer has security issues in mind in the design.
Second concern:

[2]IPV6 over Low Power Wireless Personal Area Networks
[3] User Datagram Protocol
[4]Datagram Transport Layer Security
[5]Message Queuing Telemetry Transport
[6]Constrained Application Protocol
[7]Standard Marine Communication Phrases
[8]Extensible Messaging and Presence Protocol

ISSN- 2394-5125 VOL 09, ISSUE 01, 2022

Many of these devices do not have access to security settings and the operating system. We can easily install our desired security programs on a computer or smartphone, but what to do with a smart refrigerator that has neither a keyboard nor a display?
solution:
The contents of your refrigerator may not be attractive to any hacker. But when it comes to your business information, security is a key factor. Therefore, provide only tools whose penetration routes are secure.
Of course, the concern about the lack of a display is unfounded in many cases, because all smart devices rely on software that enables interaction and personalization through your smartphone or computer.
Third concern:
Some look at the whole system with pessimism: "The onslaught of all these smart devices connected to the Internet is to gather the details of our lives!".

Solution:

Firstly, we would like to remind you that a lot of our personal, spatial, professional and other information is already received and registered through internet servers, applications, websites, social networks in which we are a member, and so on. A simple messenger program has access to your personal information, your contact information, your location, your camera and speaker. But should this application also have access to your bank account information? The point is here! In general, read about any program or device that you prepare. In the rules and regulations section, it is written what information this product collects for efficiency. If something irrational is observed, reconsider it.
Fourth concern:
Operating systems and software are alive with constant updates! Although these updates are sometimes difficult, they also ease our mind about product security. Manufacturers of smart products are divided into two categories. Those who guarantee their product has an update patch and those who find it time consuming and give it up.
solution:
The solution is clear! Get your product from the first category and also consider that the process of updating the product is not a distress.
Fifth concern:
Remote control!
Unfortunately, some manufacturers do not consider updating or security issues, yet boast the ability to remotely control their product! If home or work items can be controlled remotely, why can't a hacker do that?
solution:
We repeat the previous cases again! Only provide safe and reliable equipment to ensure your safety. To save lives, also activate the ability to remotely control important tools only when you urgently need them and block this feature in other cases.

IoT-specific security challenges:

The following is a focus on IoT-specific security challenges.
Due to the differences between IoT equipment’s and traditional computers and computer equipment, there are different security challenges that are mentioned below.

- Large-scale: Many IoT devices (such as sensors), for use on a very large scale, are far beyond traditional Internet-connected devices, so the number of links between these devices will be very large. Internet-related objects and strategies require new considerations.

ISSN- 2394-5125 VOL 09, ISSUE 01, 2022

- Homogeneous equipment and protocols: Many IoT scenarios involve a set of identical or similar devices. This homogeneity and the use of a large number of devices with the same specifications increases the potential for security vulnerabilities.
- Long-term support: Managing and supporting long-term IoT equipment is a major security challenge. In fact, unlike computers, which are designed to be able to update their software over time to deal with security threats, it is difficult or impossible to reconfigure and update IoT equipment and do not have long-term support. Also, many IoT devices are deliberately designed in such a way that they cannot be upgraded or the process is very difficult and impractical. This makes them vulnerable over time as new security threats emerge, even when adequate security mechanisms are in place at the time of production.
- Concealing the internal operation of the equipment from the user's view: Many IoT devices operate in such a way that the user has no control over the internal operation of the equipment or the data stream it generates. Actually, in practice, a device may not do what the user imagines or collect more data without user wants. This will pose a security vulnerability.
- Physical access: In some cases, IoT equipment is used in situations where it is difficult or impossible to provide physical security. In this case, hackers will have direct physical access to them. Therefore, it is necessary to see the features of Antitamper and new designs to ensure security.
- Security Standards: Early Internet of Things models assumed that this domain would be the product of private or public technology organizations. But with the growth of the Arduino and Raspberry Pi development associations, it looks like in the future every user will be able to implement their own IoT scenarios. Under these circumstances, security standards may not be applied as required.

  Ensuring the security of Internet services and applications is a very important factor for building trust among users for using this platform. Users need to make sure that the Internet, its applications, and the equipment connected to it are secure enough to perform online activities against threats. The Internet of Things is no exception to this rule, and security in this area is tied to users' trust in their surroundings. If people do not make sure that their equipment and information are reasonably secure against damage and misuse, this lack of trust will lead to a reduction in the use of IoT-based applications. In fact, in recent years, ensuring security in IoT services and products has been one of the first priorities in the development of this field and has been highly regarded.

  On the other hand, respect for rights related to confidentiality is a prerequisite for building trust on the Internet. In the field of Internet of Things, we face challenges that will be addressed below. The IoT is often referred to as a large network of sensor-equipped devices designed to collect data from their surroundings (including data related to individuals).

  In fact, as the number of Internet-connected devices in IoT-based applications increases, the likelihood of security vulnerabilities increases. Equipment that is weak in terms of security can be the starting point of cyber-attacks because they allow hackers to reprogram the equipment to prevent the system from functioning properly. This equipment may also be used to steal users' data. In addition, such equipment can create security vulnerabilities. These challenges are greater for small, inexpensive, and ubiquitous IoT applications than for computers traditionally used on the Internet. Limitations on the cost and technical dimensions of building IoT equipment force equipment manufacturers in this area to sometimes fail to meet adequate security standards, which in turn creates security and management vulnerabilities.

  In addition to the security vulnerabilities, the large number of IoT devices and their nature can increase the likelihood of an attack. Specifically, because there are usually too

ISSN- 2394-5125 VOL 09, ISSUE 01, 2022

many connections between the equipment of an IoT user, the presence of poorly secure equipment will not only affect locally, but also compromise the security and reliability of the system as a whole. For example, a refrigerator or TV infected with malware can send thousands of malicious spam emails to recipients around the world via Wi-Fi.

Today, our daily activities depend on equipment or systems that have the ability to connect to the Internet. Also, many manufacturers offer their products with the ability to connect to the Internet. Therefore, IoT equipment is needed day by day for essential services, and through it, the security of this equipment becomes more prominent. This level of dependence on IoT equipment and Internet services will increase the hackers' access to the equipment. We may be able to easily turn off an Internet-connected TV in the event of a cyber-attack, but turning off a smart electricity meter, traffic control system, or heart rate monitor implanted in a patient's body is not easy. This is because the security of IoT equipment and its services is a key issue in this area.

In fact, the security of a device is a function of the risk it faces, the damage that this risk causes are the time and resources required to achieve an acceptable level of protection. If a user uses a sensitive service that cannot withstand a high degree of security risk (such as traffic control, Internet-connected medical equipment), it is necessary to devote a significant amount of their resources to protect their system or equipment. If a user does not have a serious security concern (for example, the fact that the refrigerator connected to the user's Internet is hacked and can send spam messages), they may not be willing to pay much to buy complex security designs.

Many factors are influential in assessing security risks and ways to deal with them. These factors include: accurate identification of current and future security risks of the system, estimation of financial and non-financial costs if these risks are implemented, and estimation of cost reduction of security risks. It should be noted that the cost of making a device more secure, since the equipment is interconnected in an overall IoT ecosystem, means providing security for the entire system.

Conclusion and Discussion

As already stated, the only obstacles to the advancement of the Internet of Things are data security and privacy. At all levels of the IoT, security is essential to its proper functioning. Until today, many achievements have been made that have alleviated security concerns and provided effective implementation of the security infrastructure for the Internet of Things. In order for the IoT to be able to block its enemies and provide secure services to billions of devices of the next generation, the parameters of this research need to be further expanded and new security solutions need to be considered. Achieving privacy and security standards should also be done through basic research and the remaining questions in this research should be answered. In this study, security goals and challenges as well as IoT problems were discussed. In the future, authentication, risk assessment, and intrusion detection techniques should be addressed in each layer architecture, along with security infrastructure and IT security features. Appropriate regulatory frameworks and policies should also be in place to ensure the sustainable development of secure technologies.

There is a lot of research being done on the Internet of Things and the subject of IoT will soon become a reality. However, when this large network of interconnected devices, such as car-to-car and inter-vehicle communication, exists, new security and privacy issues and theories will emerge, and all interconnected devices will be at high risk for hackers. Because hackers are waiting for security vulnerabilities to force devices to take any action they want.

There is also a lot of large-scale debate over agreement on this issue, but it seems to have no future without successfully resolving the security threats. Due to their easy access to objects, they can easily be used by hackers at any time. Because these devices are connected to the daily lives of users, security

should be a top priority. There must be a number of security infrastructures to limit and resist threats, their availability and security.

References

[1]. Finkenzeller, K., (2003) RFID Handbook, Wiley.
[2]. Jules, A., (2006), RFID security and privacy: a research survey, IEEE Journal on Selected Areas in Communications 24(2): 381–394.
[3]. Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., Cayirci, E., (2002), Wireless sensor networks: a survey,Computer Networks 38 (4): 393– 422.
[4]. Marrocco, G., Occhiuzzi, C., Amato, F., (2009), Sensor–oriented passive RFID, In Proceedings of TIWDC,Pula, Italy.
[5]. Intel research, <http://seattle.intel–research.net/wisp/>.
[6]. http://www.gartner.com/newsroom/id/2905717 [Accessed on 21 June, 2015]
[7]. Sebastian, S. & Ray, P. P. (2015) Development of IoT Invasive Architecture for Complying with Health ofHome. In Proceedings of I3CS, Shillong, 79–83.
[8]. Sebastian S. & Ray, P. P. (2015) When Soccer Gets Connected to Internet, In Proceedings of I3CS, Shillong,84–88.
[9]. Xue Yang, Zhihua Li, ZhenminGeng, Haitao Zhang, A Multilayer Security Model for Internet of Things, inCommunications in Computer and Information Science, 2012, Volume 312, pp 388-393
[10]. Rafiullah Khan, Sarmad Ullah Khan, R. Zaheer, S. Khan, Future Internet: The Internet of ThingsArchitecture, Possible Applications and Key Challenges, in 10th International Conference on Frontiers ofInformation Technology (FIT 2012), 2012, pp. 257-260
[11]. Shi Yan-rong, Hou Tao, Internet of Things key technologies and architectures research in informationprocessing in Proceedings of the 2nd International Conference on Computer Science and ElectronicsEngineering (ICCSEE), 2013
[12]. Daniele Miorandi, Sabrina Sicari, Francesco De Pellegrini and ImrichChlamtac,Internet of Things: Vision,applications and research challenges, in Ad Hoc Networks, 2012, pp.1497-1516
[13]. Luigi Atzori, Antonio Iera, Giacomo Morabito, The Internet of Things: A Survey, in Computer Networks,pp. 2787-2805
[14]. Mr. Ravi Uttarkar and Prof. Raj Kulkarni, Internet of Things: Architecture and Security, in InternationalJournal of Computer Application, Volume 3, Issue 4, 2014
[15]. Mike Burmester and Breno de Medeiros, RFID Security: Attacks, Countermeasures and Challenges.
[16]. Benjamin Khoo, RFID as an Enabler of the Internet of Things: Issues of Security and Privacy, in IEEEInternational Conferences on Internet of Things, and Cyber, Physical and Social Computing, 2011
[17]. AikateriniMitrokotsa, Melanie R. Rieback and Andrew S. Tanenbaum, Classification of RFID Attacks.
[18]. Lan Li, Study on Security Architecture in the Internet of Things, in International Conference onMeasurement, Information and Control (MIC), 2012
[19]. John R. Douceur, The Sybil Attack, in Peer-to-Peer Systems - IPTPS, 2002, pp. 251-260
[20]. Nadeem Ahmad, Salil S. Kanhere and Problem in Wireless Sensor Network: ASurvey, in Mobile Computing and Communications Review, Volume 1, Number 2
[21]. TapalinaBhattasali, RituparnaChaki and Sugata Sanyal, Sleep Deprivation Attack Detection in WirelessSensor Network, in International Journal of Computer Applications, Volume 40, Number 15, 2012
[22]. Dr. G. Padmavathi, Mrs. D. Shanmugapriya, A survey of ATtacks, Security Mechanisms and Challenges inWireless Sensor Networks, in International Journal of Computer Science and Information Security, Volume 4,Number 1, 2009

[23]. Priyanka S. Fulare and Nikita Chavhan, False Data Detection in Wireless Sensor Network with Secure Communication, in International Journal of Smart Sensors and AdHoc Networks (IJSSAN), Volume-1, Issue-1,2011

[24]. Rabi Prasad Padhy, Manas Ranjan Patra, Suresh Chandra Satapathy, Cloud Computing: Security Issues and Research Challenges, in International Journal of Computer Science and Information Technology & Security(IJCSITS).

[25]. Bhupendra Singh Thakur, Sapna Chaudhary, Content Sniffing Attack Detection in Client and Server Side:A Survey, in International Journal of Advanced Computer Research, Volume 3, Number 2, 2013

[26]. V. Zhang, B. Qu, Security Architecture of the Internet of Things Oriented to Perceptual Layer, inInternational Journal on Computer, Consumer and Control (IJ3C), Volume 2, No.2 (2013)

[27]. E. Emam, F.K. Dankar, Protecting Privacy Using Anonymity, in Journal of the American MedicalInformatics Association, Volume 15, Number 5, 2008

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

[29]. T. Karygiannis, B. Eydt, G. Barber, L. Bunn, T. Phillips, Guidelines for Securing Radio FrequencyIdentification (RFID) Systems, in Recommendations of National Institute of Standards and Technology

[30]. Buettner, M., Greenstein, B., Sample, A., Smith, J. R., Wetherall, D., (2008), Revisiting smart dust withRFID sensor networks, In Proceedings of ACM HotNets, Calgary, Canada.

[31]. Deugd, D. S., Carroll, R., Kelly, K., Millett, B., Ricker, J., SODA: service oriented device architecture,IEEE Pervasive Computing 5 (3): 94–96.

[32]. Pasley, J., How BPEL and SOA are changing web services development, IEEE Internet Computing 9 (3):60–67.

[33]. Spiess, P., Karnouskos, S., Guinard, D., Savio, D., Baecker, O., Souza, L., Trifa, V., (2009), SOA–basedintegration of the internet of things in enterprise services, In Proceedings of IEEE ICWS, Los Angeles, Ca, USA.

[34]. Sommer, S., Scholz, A., Knoll, A., Kemper, A., Heuer, J., Schmitt, A., (2009), Services to thefield: an approach for resource constrained sensor/actor networks, In Proceedings of WAINA, Bradford, UnitedKingdom.

[35]. OASIS, Web Services Business Process Execution Language Version 2.0, Working Draft,<http://docs.oasis–open.org/wsbpel/2.0/ wsbpelspecificationdraft.pdf>.

[36]. Hydra Middleware Project, FP6 European Project, <http:// www.hydramiddleware.eu>.

[37]. Duquennoy, S., Grimaud, G., Vandewalle, J. J., (2009), The web of things: interconnecting devices withhigh usability and performance, In Proceedings of ICESS, HangZhou, Zhejiang, China.