Internet of Things (IoT): A Basic Concept and Analysis Security Issues

Pensri Pukkasenung

Faculty of Science and Technology, Rajabhat Rajanagarindra University
Chachoengsao Thailand

pensripuk@rru.ac.th

***Abstract*— The internet of things (IoT) is a huge dynamic global network infrastructure of internet enabled physical and virtual objects to connecting on concept as anything, anytime, anyplace, any place and anyone. In this paper review, analysis and briefly about IoT environment which consists of IoT definitions, elements, characteristics, architectures, technologies, application domains, and analyze the security issues and challenges.**

Keywords—IoT concept, IoT definitions, IoT elements, IoT characteristics, IoT elements, IoT architecture, IoT technologies, IoT Applications , IoT Security issues and challenges

I. INTRODUCTION

The Internet of Things is a concept of connecting many devices and people on the world to the Internet. By enabling everything "Things" to communicate send information to each other automatically. Not limited to space, place and time (anything anytime anyplace and any the related entities: see Fig. 1). Thus, IoT is a huge dynamic global network infrastructure of Internet-enabled physical and virtual objects/entities with web services which contains embedded technologies and all types of information devices such as global positioning system (GPS), infrared devices, scanners, radio frequency identification (RFID) tags/devices, sensors, actuators, smartphones, and the Internet to sense, identify, locate, track, connect, monitor, manage, communicate-interact, cooperate, and control of objects/things in physical, digital, and virtual world[1].

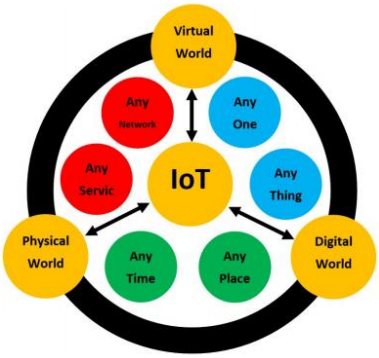

Fig. 1. Internet of Things (Io) with is connections and related entities[1].

The basic principles of IoT are 1) To make smart objects can analyze or synthesis to automatically decide what to do. 2) To facilitate the users in various ways such as making the house smart or called a smart home by controlling the electrical switch in the house, air conditioning switch control optimizing the temperature in the house, detecting smoke in the event of a house fire and ordering items for additional use in place of people in the event of a lower volume, etc. Currently, IoT applications applied into many groups for support the life living. There are related smart home, smart grid, smart city, smart healthcare, smart wearables, smart agriculture, smart transportation/mobilities, smart manufacturing/ industries, and smart supply chain. As before long, IoT will play an increasingly important role in people's daily life, from waking up to going to bed. When technology is connected to human lifestyles, it would completely change the way of living of people in this world.

According to statistics [2] reported by the Statista Research Department founded that at the end of 2018, there were approximately 22 billion IoT connected devices worldwide. And there is likely to continue to increase, forecasts suggest that by 2030, approximately 50 billion IoT devices will be used worldwide, which devices that span everything from smartphones to appliances in the kitchen, which currently has 4,550 million internet users worldwide. From the total world population of 7,750 million people, accounting for 59 percent, which has a consistently high ratio. This further reinforces that the trend of using the IoT system will also be great [3].

All devices are connected under an IoT environment consisting of sensoring, communication, computation, services, and semantics, which are performed in three main areas such as input, process data according to order and presenting information to be utilized in different ways. Therefore, all 3 operations are under diverse environments and the complexity of technology, methodology, rules and regulations for connecting to the IoT system: interoperability, heterogeneous, various models and complexity. Complexity of IoT system leaded to risk and danger that will occur in the IoT system. This will affect the security of the entire system in terms of confidentiality, integrity, availability, authentication, non-repudiation and privacy. which, if the IoT system lacks security, users will lose confidence in use because of insecurity in life and property. Therefore, countermeasures must be taken in a method for securing applications at all levels to increase efficiency and confidence for current and future users.

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

In this paper review and analyze/brief a basic concept of IoT contexts and analyze the IoT security issues and challenges. The rest of the paper is organized as follows. In Section II, IoT definitions, Section III, IoT characteristics, Section IV, IoT elements, Section V, IoT architectures, Section VI, IoT technologies, Section VII, IoT application domains, Section VIII, IoT security issues and challenges, and The conclusion is given in Section IV.

II. IoT DEFINITIONS

Back in 1999, Mr. Kevin Ashton who worked at the Massachusetts Institute of Technology, or MIT, was invited to give a lecture to Procter & Gamble, or P&G, where he presented a project called Auto-ID Center, which builds on RFID technology. At that time, it was the world standard for RFID sensors that they can connect to each other via his Auto-ID system. At the time when he presented for P&G, Mr. Kevin Ashton used the word "The Internet of Things" in his lecture slides was first defined. He defined that whatever electronic device that could communicate with each other was "Internet-like" or in simply, was an electronic device that communicates in the same way as the Internet itself. The word "things" is a term used for those electronic devices. In addition, researchers have various defined them as follows:

1) The International Telecommunication Union (ITU)[4]. defines the internet of things as a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.

NOTE 1 – Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled.

NOTE 2 – From a broader perspective, the IoT can be perceived as a vision with technological and societal implications.

2) The European Research Cluster on the Internet of Things— IERC[5]. defines the IoT as A dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual 'things' have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network.

3) Sarra et al.[6]. define The Internet of Things is a set of heterogeneous connected devices that collaborate with the Internet of services via the communication protocols. The communication protocols are importantly dedicated to the IoT devices' constraints. Mainly, this col-laboration aims to offer services needed by the end user. The IoT's services have the full potential to cover diverse domains.

4) IEEE[7]. An IOT is a network that connects uniquely identifiable "Things" to the Internet. The "Things" have sensing/actuation and potential programmability capabilities. Through the exploitation of unique identification and sensing, information about the "Thing" can be collected and the state of the "Thing" can be changed from any where, any time, anything.

The author define IoT as follows: The Internet of Things is a set of heterogeneous connected devices that collaborate with the Internet of services via the global network Infrastructure. Which self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual 'things' have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network.

III. IoT CHARACTERISTICS

The author analyze the characteristics of IoT[8-15] by extract the information through five phase of IoT lifecycle as Firstly, create phase, where devices or sensors collect information from the physical environment around them. The data from smart connected devices can be used to generate insights that can help businesses, customers and partners,; secondly, communicate phase, where the data and events generated are sent through the network to the desired destination; thirdly, aggregate phase, where data collected are aggregated by devices itself; fourthly, analyze phase, where, upon further sophisticated analytics the aggregated data can be used to generate basic patterns, control and optimise processes and finally, act phase, where suitable actions are performed based on the information created[11].

The IoT is a complex system with a number of characteristics. Its characteristics vary from one domain to another. Some of the general and key characteristics identified that founded in various researcher paper demonstrate in Table I. IoT concept focus on Interconnectivity-everything on IoT ecosystem can be interconnected with the global information and communication infrastructure as described below:

1. Connectivity: With everything going on in IoT devices and hardware, with sensors and other electronics and connected hardware and control systems there needs to be a connection between various levels.

2. Heterogeneity: All devices in the IoT system base on different hardware platforms and networks. But they can connected with other devices or services platforms through different networks.

3. Dynamic changes/self-configuring: The device state in the IoT system change dynamically as new devices are added. Automatic installation can work at all.

4. Enormous scale/Large Scale /Scalability: The number of devices that connected in the IoT system is increasing day by day. So IoT scale is big. The system able to be managed to operate effectively.

5. Things-related services/data/sensing: Consists of data that generate from the sensor and the various services in the IoT system

6. Intelligence: IoT devices and the intelligence gathered from big data analytics (also artificial intelligence).

7. Safety/security: IoT devices are connected via the global network and naturally vulnerable to security threats. Securing the endpoints, the networks, and the data moving

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

across all of it means creating a security paradigm that will scale.

TABLE I. KEY CHARACTERISTICS IN IOT

Paper [no.]	Characteristics of IoT						
	1	2	3	4	5	6	7
8	✓	✓	✓	✓	✓	✓	
9	✓	✓	✓	✓	✓	✓	
10	✓	✓	✓	✓	✓	✓	✓
11	✓	✓	✓	✓	✓	✓	✓
12	✓	✓	✓	✓	✓	✓	✓
13	✓	✓	✓	✓	✓	✓	✓
14	✓	✓	✓	✓	✓	✓	✓
15	✓	✓	✓	✓	✓	✓	✓

Characteristics:
1.Connectivity, 2. Heterogeneity, 3. Dynamic/self-configuring,
4. Enormous scale, 5. Things/services, 6. Intelligence,
7. Safety/security

IV. IOT ELEMENTS

The basic of IoT elements divided to six main elements for manage IoT activity and provide service as shown in Fig. 2. These analyze form [16][17] then conclude the IoT elements composed of identification, sensing, communication, computing, services and semantic.

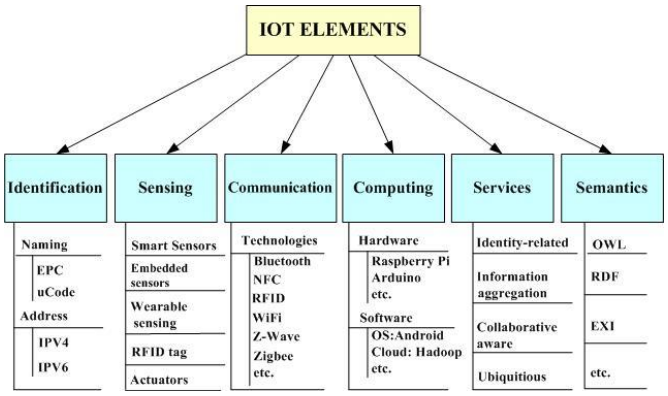

Fig.2. IoT elements

The details of IoT elements as follows:

1. Identification meaning the name(ID**)** and address of the object on the IoT system. It is very crucial which discover object in the IoT environment. Identification is the unique address of a particular object.

2. Sensor is a device that detects information from nature. And then converting the data into electrical signals for processing in the IoT ecosystem. Sensors device collects the data and send it back to storage media (database or cloud) IoT sensor have a various type and subtype such ah motion position environment mass measurement and biosensor. The details are as shown in Table II[18].

3. Communication in IoT system is the act of transferring information from one person or one place to another base on interconnection. IoT communication technology connect device using the different protocol such as Bluetooth, WiFi, RFID, Near Field Communication (NFC).

TABLE II. IOT SENSOR TYPES AND SUBTYPES

Type	**Motion**	**Position**	**Environment**	**Mass Measurement**	**Biosensor**
Subtype	Movement	Orientation	Temperature	Volume	Blood
	Velocity	Inclination	Humidity	Pressure	Organ
	Inertia	Proximity	Luminance	Density	Mental
	Vibration	Presence	Acoustic	Deformation	Tissue
	Acceleration	Location	Radiation	Viscosity	
	Rotation		Gas	Flow	
			Magnetic Field	Load	
			Weather	Moisture	
			Chemical	Shock	
			Electrical	Contact	
			Color	Strain	
			EMF[2]	Corrosion	
				Electrical Conductivity	
				Oxygen	

4. Computation was operated by processing unit (hardware: processor) and software application. Processing unit mostly work on real-time basis and gives intelligence to the data for decision making. IoT application run on various hardware platforms and software platforms play an important role to perform the processing. Processing unit and software application are the main process on IoT system there are the brain of the IoT.

5. Services on IoT system can be categorized under four classes: Identify-related service, information aggregation service, collaborative service and ubiquitous services Identity-related services connected everything in the physical world to the virtual world to have the objects identified. Information aggregation services in corporate identity related services and monitoring the situation of IoT environment. Collaborative-aware services use of the data collected to make decisions and perform actions Ubiquitous service are the ultimate aimed of the Internet of Things, taking collaborative-aware services to providing complete access and control of every-thing around us through a computer or a mobile phone or something else.

6. Semantic services exacted the knowledge, include identifying and analyzed data for decision making

V. IOT ARCHITECTURES

The author analyzed the layer of existing architecture from research paper [19-28] focus on the responsibility and selected 7-layers suitable for IoT layer architecture which consists of perception layer, network layer, middleware layer, application layer, business layer, security layer, and management layer. The details which explain of each layer as follow:

1. Perception layer: the perception layer is responsible for detecting, collecting, processing information and transmitting it to the network layer. Through sensors and other IoT devices under various protocols

2. Network Layer: the network layer is responsible for connecting to all objects or devices in IoT environment. Its features are also processing data and transmit to the other layer. Its includes network communication software and physical components such as protocols, gateway, routing and addressing.

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

3. Application layer: the application layer is responsible for defines software or application that use the IoT technology. The applications function consists of data formatting, presentation, things services to users according to their needs. The applications of IoT can be smart homes, smart cities, smart health, animal tracking, wearable etc.

4. Support layer/processing layer/middleware layer: the responsible of this layer will be an integral all parts of the processing of huge amount of information. more efficient by applying cloud computing and fog computing technology which suitable for the currently situation. many IoT architectures extended to this layer.

5. Business Layer: the responsible to manage and control application and business logic led to the business success model.

6. Security Layer: the responsibility of security layer focus on the protection of IoT assets, these ensure in security issues cover all layers in IoT environment. The properties of security issues consist of confidentiality, Integrity, availability, authentication, non-repudiation , and privacy.

7. Management Layer: the responsible of this layer monitoring and controlling whole IoT system focus on IoT devices , QoS management, Trust& reputation management, security management service management, network management etc. Summary the responsibility of each layer show in Table III. and Fig. 3. demonstrated a layer concept.

TABLE III. SUMMARY THE RESPONSIBILITY OF LAYER

Layer	Responsibility
Perception layer	detecting, collecting, processing information and transmitting it to the network layer. Through sensors and other IoT devices under various protocols.
Network layer	connecting to all objects or devices in IoT environment. Its features are also processing data and transmit to the other layer. Its includes network communication software and physical components such as protocols, gateway, routing and addressing.
Middleware layer	processing of huge amount of information. more efficient by applying cloud computing and fog computing technology
Application layer	defines software or application that use the IoT technology. The applications function consists of data formatting, presentation, things services to users according to their needs. The applications of IoT can be smart homes, smart cities, smart health, animal tracking, wearable etc.
Business layer	manage and control application and business logic led to the business success model.
Security layer	protection of IoT assets, these ensure in security issues cover all layers in IoT environment. The properties of security issues consist of confidentiality, Integrity, availability, authentication, non-repudiation , and privacy
Management layer	monitoring and controlling whole IoT system focus on IoT devices , QoS management, Trust& reputation management, security management service management, network management etc.

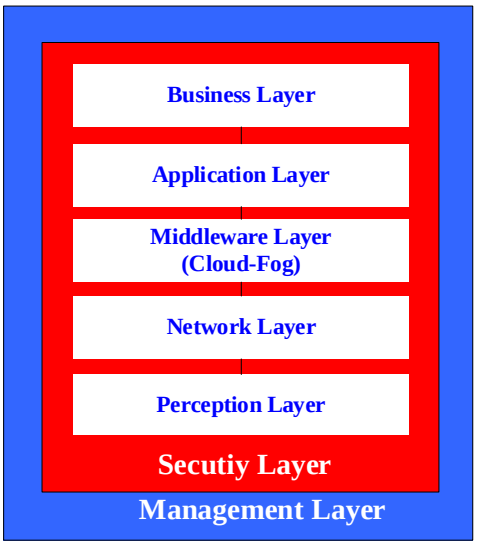

Fig. 3. Layer of IoT architecture concept

VI. IoT TECHNOLOGIES

With a various of devices connected in the IoT system Therefore, communication models have been developed a wide variety of applications. Which is the origin of many protocols or technologies in IoT environment. Protocols or technologies are classified into five groups for Communications divided by distance and size up various wireless protocol candidates for IoT applications is by the projected range of their connections. Fig. 4. [29][30]. Detail technologies are described in the following as below:

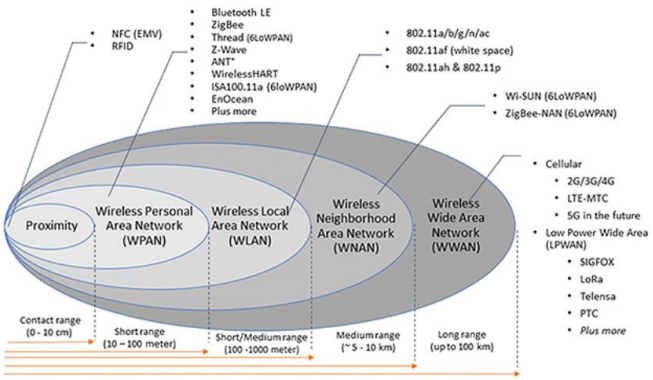

Fig. 4. IOT Technology divided by distance and projected range [1]

- *A Proximity:* Contact rang 0-10 cm such as technology NFC (near-field communication and RFID (radio frequency identification). Both employ radio signals for all sorts of tagging and tracking purposes, sometimes replacing bar codes. NFC is still an emerging technology; RFID, however, is currently in widespread use all over the world[31]. For example applications are contactless payment and identity and access.

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

- *A WPAN (Wireless Personal Area Network):* Short range 10-100 meter such as technology Bluetooth, ZigBee, Z-Wave, 6LoWPAM etc. These design for a personal area network that interconnecting devices centered around an individual person's workspace such as the automatic control system in the home (Home Automation) that connected all electronic devices together. For Example of the application in this network include of automotive, home automation, smart grid, remote control, smoke alarm and security sensors[32].
- *A WLAN (Wireless Local Area Network):* Short/medium range (100-1000 meter)-a network that connects two more devices using a wireless distribution method and provides access to the public internet. Most WLANs are based on Institute of Electronic and Electronic Engineers (IEEE) 802.xx Standard such as 802.11a/b/n/ac, 802.11af, and 802.11ah, 802.11p, otherwise known as Wi-Fi[33]. For example of these applications are wearable devices or extend range ,wireless access in vehicle environment (Wave) and target for internet of things[32].
- *A WNAN (Wireless Neighborhood Area Network):* Medium range (5-10 km) such as technology standard Wi-SUN (6LOWPAN) and ZigBee-NAN (6LOWPAN). These designed base on IoT devices that connected with wireless area network and supported IPV6.
- *A WWAN (Wireless Wide Area Network):* Long range up to 100 km- it is looks like a wireless network but designed specific for a larger size of a wide area network. WWAN are network traffic support a mobile communications technology such as worldwide interoperability. For example, Cellular (2G/3G/4G), LTE-MTC, 5G, and Low Power Wide Area (SIGFOX, LoRa, Lelensa, PTC). Target applications: smart meter, smoke detector, agriculture, street lighting, parking, social housing, pet tracking, garbage collection, forest fire detection etc[32].

VII. IoT Application Domains

Currently, IoT application domains focusing on 9 groups consists of smart manufacturing/industrial, smart transportation/mobility, smart grid/energy, smart retail, smart cities, smart healthcare, smart supply chain, smart agriculture, and smart building/home. All concept as shown in Fig. 5.

IoT applications are being used more and more, according to statistics which analyze by The IoT analytics [34]. Analysis of the top IoT application areas in 2020 shows that of the 1,414 public enterprise IoT projects identified,

Fig. 5. Application domains

manufacturing / industrial settings are most common (22%), followed by Transportation / mobility (15%) , energy IoT projects (14%), retail 12%, cities 12%, healthcare 9%, supply chain 7%, agriculture 4%, buildings 3% and the other 3% see Fig. 6.

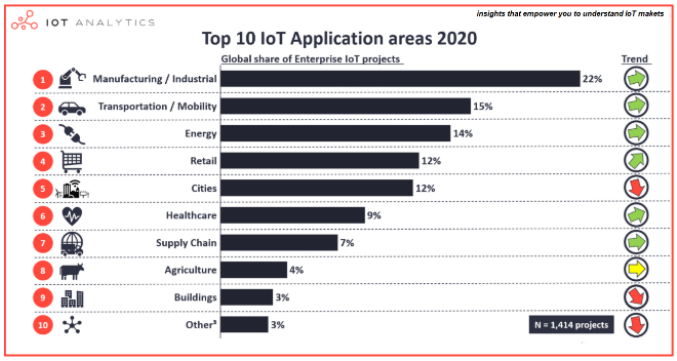

Fig. 6. Top 10 IoT application areas 2020[34]

From Fig. 6. was founded six applications are increasing volume, while four applications are stable and decreasing. There are compared with analytics IoT application analysis 2015 and the 2018 analysis.

The details of IoT application and functions as follows:

1. *Smart manufacturing/industrial:* it well known in smart factory which included another incentive in assembling unrest by coordinate's man-made brainpower, AI, and robotization of information work and M2Mcommunication with the assembling procedure. The smart factory will on a very basic level change how items are created, fabricated and transported. Simultaneously it will improve laborer safety by empowering low discharges and low episode fabricating. These advances in the manner machines and different items convey and the subsequent manner by which dynamic moves from people to specialized frameworks implies that assembling becomes "more astute". new advances such; Automation, mechanical technology, and independent versatility are all gives a methods for brilliant assembling yet M2M communications empowered by the "modern" IoT will gives a full importance of smart factory and manufacturing by the method of Big Data

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

idea which in this specific situation, refers to the scientific prospects offered by the volume and assortment of information that is created by an organized economy to enhance the mechanical procedures to suggesting less support vacation, less blackouts and much reduced energy consumption[35].

2. Smart transportation/mobility: Transportation is the important elements to show the prosperity of the nation. A road condition checking and ready application is progressively significant of IoT change application. The primary idea of smart transportation and mobility is to apply the standards of publicly supporting and participatory detecting. The procedure started with client distinguished the course wishes and denoted a few focuses as pothole in the PDA's application. The smart transportation is managing three primary originations such as transportation systematic, transportation control, and vehicle network. The routing of vehicles and speed control are completely known as transportation control which they quite identified with the method of the vehicles network and by and large represented by multi-innovation.[35].

3. Smart grid/energy: IoT can support technologies in SG. Comprehensive sensing and processing abilities of IoT can improve SG abilities such as processing, warning, self-healing, disaster recovery, and reliability. Combining IoT and SG can greatly promote the development of smart terminals, meters and sensors, information equipment, and communication devices. IoT can be used to accomplish reliable data transmission in wire and wireless communication infrastructures in different parts of SG(electricity generation, transmission lines, distribution, and consumption/utilization) as follows: 1) In electricity generation, IoT can be used to monitor electricity generation of different kinds of power plants (such as coal, wind, solar, biomass), gas emissions, energy storage, energy consumption, and predict necessary power to supply consumers. 2) IoT can be used to acquire electricity consumption, dispatch, monitor and protect transmission lines, substations, and towers, manage and control equipment. 3) IoT can be used in customer side in smart meters to measure different types of parameters, intelligent power consumption, interoperability between different networks, charging and discharging of electric vehicles, manage energy efficiency and power demand[37].

4.Smart retail: it have many functions that help the business so powerful such as automated checkout to ease payments that could be even totally hands-free, and to reduce queuing times to provide a better customer experience, real-time in store marketing through proximity-activated promotions that push notifications in our smartphones or wearables, and personalized CTA's on digital signage, among others, store layout optimization as a result of consumers' behavioral data analysis and identification of hotpots and hottest items, less inventory shrinkage due to an improved monitoring of stocks and shoplifting, efficient energy management that would reduce fixed costs and adapt power and lighting to store's occupation at each moment, maintenance tailored to current equipment conditions instead of periodic revisions that may be either insufficient or unnecessary, Inventory optimization due to a more accurate volume forecasting and a wiser assortment based on consumers' purchasing behavior data analysis, improved staff allocation adapted to fill heavier traffic stores, areas inside the store and hours, improved employee productivity through technologies such as augmented reality to show added value information on schedule, a consumer's history, smarter CRM really laser targeted and personalized to each unique user's history with the brand can be done in real-time by facial recognition of customers, or simply by beacons acquaintance of their individual smartphones. etc[39].

5. Smart cities: it monitor and control all functions in the cities to smart cities. IoT application gives the accompanying offices in smart cities such as Efficient Water Supply with smart meters can encourage spillage identification and reduce wastage of water, Smart Traffic Management it's simpler to deal with traffic blockage with smart traffic signals, Reliable Public transportation to deal with the basic circumstance like barriers or road blocks, transportation is upset, Energy Efficient Buildings IoT development is making it less complex for building vitality proficient structure structures, Smart Management Application that controls nonstandard heating, cooling, lighting, and fire-security systems. Smart Parking utilized GPS information from PDAs and video checking can help a vehicle driver to discover a parking space, Smart Street lighting faculties or tracks the development and modifies the lighting to reduce, light up or switch off or on naturally dependent on the earth, Healthy Environment with sensors can be joined to measure the nature of the water by looking at the degree of pH, air, soil, and so on, and Waste Management IoT devices like sensors can be joined to a trash compartment that assembles the information about the degree of waste in the holder etc[35].

6. Smart healthcare : the application of smart healthcare can be grouped into inter-body sensing, intra-body sensing and environmental management. Intra body sensing applications refer to those which help in monitoring multiple vital signs. For example, in fitness tracking through a smart watch, along with parameters such as number of calories burned, steps taken, active hours etc., it is also important to track the ph sensitivity of the sweat, oxygen intake of the body, heart rate monitoring etc. Moreover, it provided the environmental management applications help in establishing communication between the hospital and the patient. Monitoring the first responder's health status in an endemic or epidemic outbreak, getting ambulance assistance in case of emergency, developing evacuation schemes for disaster management in hospitals, maintaining active databases to ensure correct delivery of organs/blood to the users in need, accurate billing of surgical procedures through RFID tags are some of the significant applications in environmental management[36].

7. *Smart supply chain:* it as a modern system
can be defined as the overall process management of goods or services involving advanced product-tracking devices and systems as the instrumentation. The scope of smart supply

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

chains goes beyond the isolated manufacturing process or system and extends to, but is not limited to, the areas of customer segmentation and omnichannel as well as time-to-market and flexible re-optimization of plans. A smart supply chain is instrumented with machine generated information, which is interconnected among various stakeholders and product/ service components at all levels and the smart supply chain is intelligent enough to analyze incredibly complex and dynamic business scenarios . The future smart supply chain will have the basic attributes of connections, collaboration, customization, and flexibility[40].

8. Smart agriculture: it as to well known in smart farming which is a hi-tech and effective system of doing agriculture and growing food in a sustainable way. It is an application of implementing connected devices and innovative technologies together into agriculture. IoT based on smart farming improves the entire Agriculture system by monitoring the field in real-time. With the help of sensors and interconnectivity, the Internet of Things in Agriculture has not only saved the time of the farmers but has also reduced the extravagant use of resources such as water and electricity. It keeps various factors like humidity, temperature, soil etc. under check and gives a crystal clear real-time observation. The following are the benefits of adopting new technology - Internet of Things in agriculture: climate conditions, precision farming, smart greenhouse, data analytic and agricultural drones[38].

*9. Smart home/smart building***:** The IoT as utilized in smart home and buildings to deal with smart function in different applications by control devices through the internet using a mobile or other network, the user to control functions such as lighting, (control interior or exterior light), shading system, (automatic control sensor and adjustable to be suitable etc.), heating(air conditioning, air quality, preparation of hot water etc.), ventilation and air conditioning, safety functions(electronic security system, electronic fire system, protections against flooding, the camera system), multimedia(control audio/video system, home cinema, hi-fi system, digital images, Voip phone, intercom or piano), health(disabled people, call for emergency medical services, drug dosage, ECG, Blood count, measurement of pressure, measuring height, skin testing, temperature, stability control ones body etc.), kitchen(no household, control the baking, delivery of goods into the house, bread machine, check water filtration system security management, check the date of the food, control of microwave, washing operation etc.), irrigation(irrigation system provides intelligent flora around the house a sufficient supply of water and nutrients that may be using drop irrigation, irrigation or spray irrigation or micro irrigation system. Irrigation using outside air conditioning can also be used for hot days in summer on the terrace.), clean(to ensure user comfort SH should ensure fewer problems with maintenance, Cleanliness in the house provides a variety of robots, central vacuum and cleaning robots for pools and bath. Clean sidewalks, gutters, roof against snow provide thermo cables), control(manageability of smart home, intelligent control of the house is possible by phone, touch, panel, remote controls. And switches, connecting via the internet or by voice)[41].

VIII. IoT Security Issues and Challenges

Everything connected to the internet for exchanging data via global network. Led to many applications in various areas such as smart home, smart city, healthcare, agriculture, logistics, vehicular technology etc. The number of devices that are expected to be connected to internet from the Gartner by 2020 is 50 billion. And the number is increasing to 500 billion by 2030[42]. Beside the Size of the Internet of Things (IoT) security market worldwide from 2016 to 2025, 7.28 to 30.9 billion U.S. dollars[43]. As shown in Fig. 7.

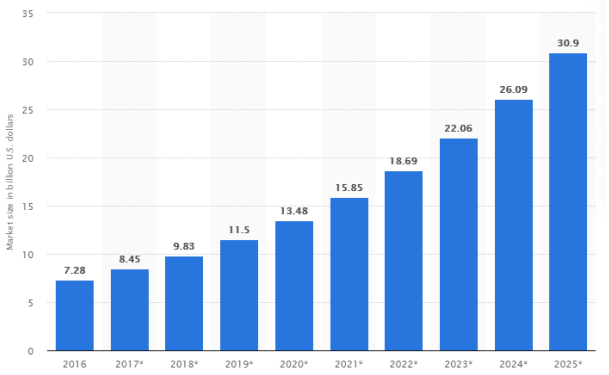

Fig. 7. The Size of the Internet of Things (IoT) security market worldwide from 2016 to 2025[43]

Along with this rising the IoT security market worldwide and enormous of devices integrated and connected to internet which the reason to concerns in an IoT environment in cybersecurity issues. The conceptual as security shown in Fig. 8.

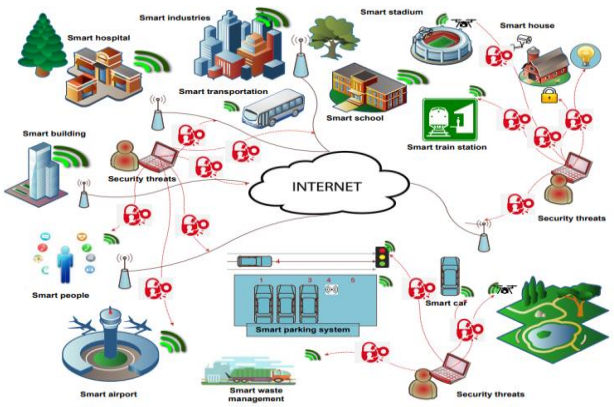

Fig. 8. Security concerns in an IoT environment[44]

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

The IoT security issues and challenges which are survey and analysis from the existing 10 research papers was described in various topic such as security service, security issues in IoT environment, main security requirements, security issues in IoT, and security parameters. The results of analyze the topic security challenges as shown in Table IV.

TABLE IV. SECURITY CHALLENGES

PaperNo,Year	Topic	Security Issues
1[45], 2016	Security Service	Authentication, Authorization, Integrity, Confidentiality, Non-repudiation, Availability, Privacy
2[46], 2016	Security Issues in IoT Environment	Confidentiality, Integrity, Authentication, Authorization, Availability, Privacy
3[47], 2016	Main Security Requirements	Confidentiality, Integrity, Authenticity, Availability,
4[48], 2017	Security issues in IoT	Access control, Privacy, Trust, Confidentiality
5[49], 2017	Security Requirements of IoT Devices	Confidentiality, Integrity, Availability, Authentication, Authorization
6[50], 2017	Security Parameters	Privacy, Availability, Integrity, Confidentiality, Authenticity
7[51], 2018	Security Services	Confidentiality, Integrity, Authentication, Non-repudiation, Availability, Privacy
8[52], 2019	Security Requirements	Availability, Authenticity, Confidentiality, Integrity, Non-repudiation, Privacy
9[53], 2019	Security Requirements	Confidentiality, Integrity, Non-repudiation, Availability, Privacy, Audibility, Accountability, Trustworthiness
10[54], 2019	Cyber Security Requirements	Identification, authentication, Authorization, Privacy, Accountability, Non-repudiation, auditing

From Table IV. The security issues consist of confidentiality, availability, integrity, non-repudiation, authentication, identification, authorization, privacy, accountability, access control, auditing, and trustworthiness. In order to show the frequency of the security issues from all selected paper the author create the relationship between the security properties and each research paper as show in Fig. 9. Then selected the most security issues or security properties to the security requirements and challenges. Finally, The author viewpoint concluded the security requirement for IoT system as follows:

- *Confidentiality:* It ensure the information can discover by the authorized persons.
- *Integrity:* It ensure the information has not been modified by the authorized persons.
- *Availability:* It guarantee the IoT system can continue to work all the most processes.
- *Authentication:* Prove identity whether a person has a the right or not. Access data by illegal users are not allowed.

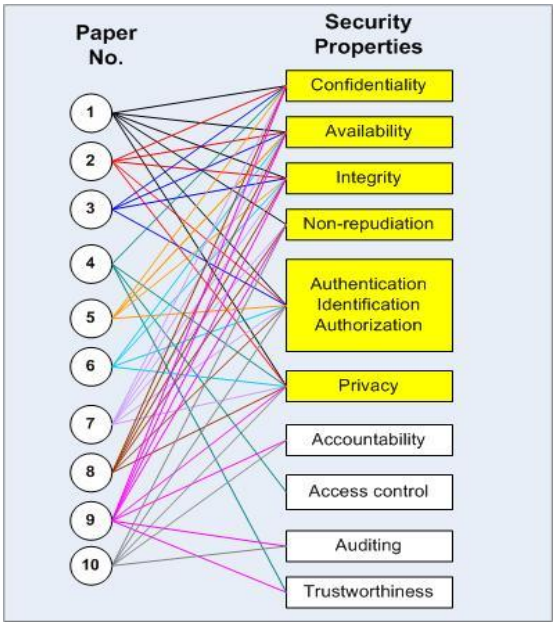

Fig. 9. The relationship between paper and security properties

- *Non-repudiation:* It ensure the sender of the information cannot refuse having sent the information in the future.
- *Privacy*: It ensure to prevent private information from being leaked to malicious entities.

The Security requirements concept as shown in Fig. 10.

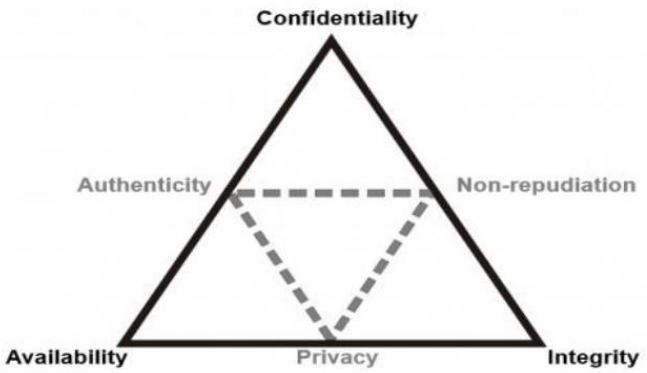

Fig. 10. Security requirements [52]

IX. CONCLUSION

In this paper review, analyzed and briefly about IoT environment with consists of IoT definitions, elements, characteristics, architectures, technologies, application domains, and analyze the security issues and challenges: Definition: The Internet of Things is a set of heterogeneous connected devices that collaborate with the Internet of services via the global network Infrastructure. Which self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual 'things' have identities,

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network, IoT Characteristics consists of 1.Connectivity, 2. Heterogeneity, 3. Dynamic/self-configuring, 4. Enormous scale, 5. Things/services, 6. Intelligence, and 7. Safety/security, IoT Elements composed of identification, sensing, communication, computing, services and semantic, IoT Architecture consists of perception layer, network layer, middleware layer, application layer, business layer, security layer, and management layer, IoT Technologies are protocols or technologies in IoT environment. Protocols or technologies are classified into five groups for Communications divided by distance and size up various wireless protocol candidates for IoT applications is by the projected range of their connections, IoT Application domains focusing on 9 domains: smart manufacturing/industrial, smart transportation/mobility, smart grid/energy, smart retail, smart cities, smart healthcare, smart supply chain, smart agriculture, and smart building/home, and IoT Security Issues emphasis on Availability, Authenticity, Confidentiality, Integrity, Non-repudiation, Privacy. The expected that this study will be use full for researchers and practitioners, helping them to understand enormous potential of internet of things and addition this to forecast the challenge of IoT which will be encountered.

REFERENCES

[1] A. Ghasempour. (2019). Internet of Things in Smart Grid: Architecture, Application, Services, Key Technlogies, and Challenges. [Online]. Available: www.mdpi.com/journal/inventions.

[2] Number of internet of things (IoT) connected devices worldwide in 2018, 2025 and 2030(in billions). [Online]. Available: https://www.statista.com/statistics/802690/worldwide-connected-devices-by-access-technology/

[3] Digital Marketing donsultancy. (2020). [Online]. Available:https://www.twfdigital.com/blog/2020/02/global-digital-usage-stat-q1-2020/

[4] ITU, Committed to connecting the world. [Online]. Available: http://www.itu.int/en/ ITUT/gsi/iot/Pages/default.aspx.

[5] Internet of Things and future internet enterprise systems. [Online]. Available: http:// cordis.europa.eu/fp7/ict/enet/rfid-iot_en.html.

[6] S. Hammoudi, Z. Aliouat, S. Harous. (2018). Challenges and research directions for Internet of Things. Springer Telecommunication Syst(2018)0. [Online]. Available: http://doi.org/10.1007/s11235-017-0343-y

[7] R. Minerva, A. Biru , D. Rotondi. (2015). Towards a definition of the Internet of Things (IoT). IEEE, 2015.

[8] Z. Ye. Internet of things.(2020). [Online]. Available : https://slideplayer.com/slide/12840354/

[9] O. V. Sintef, P. FriessEU, Belgium. (2014). Internet of Things– From Research and Innovation to Market Deployment. river publishers' series in communications, 2014.

[10] Nitsawan katerattanaku. (2020). (What is IoT? Key characteristics. [Online]. Available: https://www.i-scoop.eu/internet-of-things/ -intelligent

[11] S. Kar. (2017). Internet of Things: Characterstics, Technologies, AND Applications.[Online]. Available: https://www.slideshare.net/sutrishnakar1995/internet-of-things-iot-introduction-ppt

[12] K. Chandrashekhar. (2016). Internet of Things (IoT) Characteristics. [Online]. Available: https://www.linkedin.com/pulse/internet-things-iot-characteristics-kavyashree-g-c

[13] F. D. Oré. (2020). Characteristics Within The Internet Of Things (IOT). [Onine]. Available: https://www.reloade.com/blog/2013/12/6-characteristics-within-internet-things-iot.php

[14] H. F. Atlama,b, G. B. Willsa. (2018). Technical aspects of blockchain and IoT. [Online]. Available: https://www.researchgate.net/publication/329882609

[15] K. K. Patel1 , S. M. Patel. (2016). Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges International Journal of Engineering Science and Computing, May 2016, IJESC

[16] S.P. Raja, T. Sampradeepraj. (2018). Internet of thing: a research -oriented introductory. Int. J. Ad hoc Ubiquitous Computing, Vol. 29 Nos. 1/2 , 2018.

[17] S. Gupta, N. K. Sharma, M. Dave. (2016). internet of things: A survey on Architecture and Elements. International Journal of Engineering and Management Research. Volume-6, Issues, November-December.

[18] V. Rozsa, M. Denisczwicz, M. Dutra, P. Ghodous, C. F. Silva, N. Moayeri, F. Biennier, N. Figay. (2017).An Application Domain-Based Taxonomy for IoT Sensors.

[19] B. M., Rehman, R. Khan, B. & Kim, B. (2018). IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey. Sensors,18(9).

[20] G. D. Diana , S. ElRoda, C.E. ElManial, (2015). Improved Layered Architecture for Internet of Things. International Journal of Computing Academic Research (IJCAR) ISSN 2305-9184 Volume 4, no 4 (August 2015), pp.214-223.

[21] A. Dean, (2018). A Study of Advances in IoT Security, ISCSIC '18 , September 21–23, 2018, Stockholm, Sweden © 2018 Association for Computing Machinery.

[22] Y. T. Mahmoud, R. Aloul, F. Zualkernan. (2015). Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures. International Journal for Information Security Research (IJISR), Volume 5, Issue 4, December 2015).

[23] J. SathishKumar, R. D. Patel. (2014). A Survey on Internet of Things: Security and Privacy Issues. International Journal of Computer Applications, 90(11), 20–26.

[24] P. Sethi, S. R. Sarangi. (2017). Internet of Things: Architectures, Protocols, and Applications. Journal of Electrical and Computer Engineering, 2017, 1–25.

[25] M. Kumar, V. Suganthi, P. Manojkumar, (2019). A Literature Survey on Internet of Things security issues International Journal of Computer Sciences and Engineering Open Access Survey Paper 2019 vol: 7 (2): 139.

[26] K. P. Keyur, M.P. Sunil. (2016). Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges. International Journal of Engineering Science and Computing. Volume 6, Issues No.5.

[27] O. Vermesan, P. Friess. (2014). "IERC Cluster SRIA 2014, Internet of Things From Research and Innovation to Market Deployment". River Publishers Series in Communication.

[28] H. Rahimi, A. Zibaeenejad, A.A. Safavi (2018). A Novel IoT Architecture based on 5G-IoT and Next Generation Technologies. 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference.

[29] M. Zemede. (2015). Keysight Technologies. [Online]. Available: https://www.microcontrollertips.com/

[30] K. Naito. (2017). A Survey on the Internet-of-Things: Standards, Challenges and Future Prospects. Journal of Information Processing. Vol.25 23-31 (Jan. 2017)

[31] N. Chandler. What's the difference between RFID and NFC? [Online]. Available: https://electronics.howstuffworks.com/difference-between-rfid-and-nfc.htm.

[32] Keysight Technologies. (2015). IEEE802.154g Standard. [Online]. Available:https://www.keysight.com/upload/cmc_upload/All/Slide_IOT_Part_2.pdf.
[33] SDXCENTRAL. (2020). Wireless Local Area Network (WLAN). [Online]. Available: https://www.sdxcentral.com/resources/glossary/wireless-local-area-network-wlan/.
[34] P. Scully. (2020). Top 10 IoT Application areas. https://iot-analytics.com/top-10-iot-applications-in-2020/
[35] T. Manivannan, P. Radhakrishnan. (2020). Preventive Model on Quality of Service in IoT Applications. International Journal of Mechanical and Production Engineering Research and Development (IJMPERD) ISSN(P): 2249-6890; ISSN(E): 2249-8001 Vol. 10, Issue 3, Jun 2020, 1247–1264
[36] A. Ghasempour. (2019). Internet of Things in Smart Grid: Architecture, Application, Services, Key Technologies, and Challenges. MDPI, Inventions 2019, 4, 22. www.mdpi.com/journal/inventions.
[37] A. Sanz. (2016). The IoT Smart Retail Overview-Infographic. http://blogs.icemd.com/blog-iot-and-digital-marketing/iot-smart-retail-infographic/
[38] P. Sundaravadivel, E. Kougianos, P. S. Mohanty, M. Ganapathiraju. (2018). Everything You Wanted to Know about Smart Health Care: Evaluating the Different Technologies and Components of the Internet of Things for Better Health. IEEE Consumer Electronics Magazine 7(1):18-28.
[39] S. J. Lee, T. K. Shi. (2018). Review of Literature and Curricula in Smart Supply Chain & Transportation. [Online]. Available: https://transweb.sjsu.edu/sites/default/files/Cheng-Shi smart-supply-Chain-Curricula 1.pdf
[40] B. Intellia. (2019). IoT in agriculture , 5 applications of IoT in agriculture -making agriculture smarter. [Online]. Available: https://www.biz4intellia.com/blog/5-applications-in-agriculture/.
[41] J. Chen. (2020). Smart Home. [Online]. Available: https://www.investopedia.com/terms/s/smart-home.asp.
[42] K. Panetta. (2018). Gartner Top Strategic Predictions for 2018 and Beyond. [Online]. Available: https://www.gartner.com/smarterwithgartner/gartner-top-strategic-predictions-for-2018-and-beyond, on (28.08.2020).
[43] M. G. Samaila, M. Neto, D. A. B. Fernandes, M. M. Freire. P. R. M. Inacio. (2018). Challenges of securing Internet of Things devices: A survey. Wileyonlinelibrar.com/journal/spy2.
[44] I. Yaqoob, E. Ahmed, H. Muhammad ,U. Rehman et al. (2017). The rise of ransomware and emerging security challenges in the Internet of Things. Computer Networks December, 2017.
[45] O. E. Mouaatamid, L. Mohammed & M. Belkasmi. (2016). Internet of Things Security: Layered classification of attacks and possible Countermeasures. e-TI – Numéro 9 – 2016 – http://www.revue-eti.net – ISSN 1114-8802.
[46] R. S. Mary Joshitta, L. Arockiam. (2016). Security in IoT environment: A survey. Int. Journal of Information Technology & Mechanical Engineering -IJITME, Vol. 2 Issue. 7, July-2016, pg.1-8.
[47] A. Muhammad , G. Oladiran, A. Magdy, A. Bayoumi. (2016). A Review on Internet of Things (Iot) : Security and Privacy Requirements and the Solution Approaches. Global journal Inc. (US).
[48] J. P. Tailor, A. D. Patel. (2017). Comprehensive Survey on Security Problems and Key Techologies of the Internet of Things(IoT). International Journal of Research and Scientific Innovation (IJRSI). Volume IV, Issue VIS, June 2017, ISSN 2321-2705.
[49] S. Yoon, J. Kim, Y. Jeon. (2017). Security Considerations Based on Classification of IoT Device Capabilities. The Ninth International Conferences on Advanced Service Computing. IARIA, 2017.
[50] J. Yashaswini. (2017). A Review on IoT Security Issues and Countermeasures. Oriental Journal of Computer Science & Technology. ISSN: 0974-6471, June 2017, Vol. 10, No.(2): Pgs 454-459.
[51] D. E. Kouicem, A. Bouabdallah, H. Lakhlef. (2018). Internet of Things Security: a top-down survey. Journal of Computer Networks 141 , March 15,2018.
[52] C. Atac, S. Akleylek. (2019). A Survey on Security Threats and Solutions in the Age of IoT. Eropean Journal of Science and Technology No 15, pp. 36-42, March 2019.
[53] H. A. Abdul-Ghani, D. Konstantas. (2019). A Comprehensive Study of Security and Privacy Guidelines, Threats, and Countermeasures: An IoT Perspective. Journal of Sensor and Actuator Networks. 22 April 2019.
[54] S. Nasiri, F. Sadoughi, M. H. Tadayon, A. Dehnad. (2019). Security Requirements of Internet of Things-Based Healthcare Sysem: a Survey Study. Journal of Academy of Medical Sciences of Bosnia and Herzegovina.