SECURITY, PRIVACY AND TRUST IN IOT

NAME SATVIKA M
CLASS AI-DS(B)
REG.NO 2101110113

INTRODUCTION

Internet of Things (IoT) is the networking of physical objects that contain electronics embedded within their architecture in order to communicate and sense interactions amongst each other or with respect to the external environment. IoT is reaching new peaks and rapidly gaining momentum and popularity in many domains of our daily lives. These domains include vehicles, industry, education, agriculture, hospitals, environmental monitoring etc.Environmental monitoring, smart homes,smart grid,wearables,industrial iot, smart city,internet of vehicles and medical and health care are the applications, areas, and usage of IoT in our daily routines and lives. In every aspect, internet of things (IoT) has its marks and milestones which are gradually increasing as the technology is getting advanced and handy to use.IoT provides the services in a more effective and efficient way. However, there are some critical factors that come along with the advancement of technology,some of these factors are namely security, privacy, and trust of the end user.Security, privacy, authentication, and trustworthiness for the end users is considered to be the main feature for any technology.There are some well know projects in the field of IoT which focused on the security aspect and their comparison can be seen in fig 1. Most commonly observed requirements for IoT security are namely authentication, confidentiality and access control. There are several available ways in which security, privacy, and trust of IoT can be managed in which NFC, RFID, and WSN are commonly used.

Projects	Authentication	Confidentiality	Trust	Privacy
Butler [3]	✓	✓	×	✓
EBBITS [4]	×	✓	×	×
Hydra [5]	×	✓	×	×
uTRUSTit [6]	✓	×	✓	×
iCore [7]	✓	✓	✓	✓
HACMS	✓	✓	×	×
NSF [8]	✓	✓	✓	✓

Figure 1: Projects focusing on Iot security

TRADITIONAL INTERNET AND INTERNET OF THINGs

The first and most grasped difference between the traditional Internet and the IoT is the identity of the content creation.For example, the content in the traditional Internet is consumed by request; that is, one has to ask a query, issue a search or send a request for a web service in order to consume the content. On the contrary, in the IoT, the content is typically consumed through pushing the technology as a notification or triggering an action when a situation of interest is detected. In many cases, the consumption means combining data from different sources. This is true for the traditional Internet as well as the IoT.In the traditional Internet, the connection is done through physical links between web pages. In the IoT, the combination of data is required for situation detection. This is manifested in the combining of data in the form of context-based event patterns in which some of the data determines the context and

other determines the pattern itself.There are many more differences which are listed in the table below.

Area	Traditional Internet	Internet of Things (IoT)
Content	Human creates content	Machine creates content
Content Consumed	By generating request	By triggering actions and pushing information
Content Combined	Using links (explicitly)	Using operators (explicitly)
Data	Generate with the help of peoples	Generate with the help of sensors (e.g. Temperature, pressure)
Efficient	Increase and covers internet efficiency	Add intelligence to the procedure

Figure 2: Projects focusing on Iot security

SECURITY, PRIVACY, AND TRUST IN THE INTERNET OF THINGS

Security plays an important role in terms of usability, efficiency, and reliability in IoT. The need for privacy is the core property of self-actualization in IoT. There are several applications working in many different grounds like patient monitoring system, traffic control, energy consumption inventory management, smart parking, civil protection any many others. Privacy should be guaranteed to the end user. After security, the main aspect occurs is the privacy and with privacy, there is trust (see Fig.3), according to the internet of things, trust is also an important aspect or factor which is developed by the end user when there is an element of security and privacy in the device.

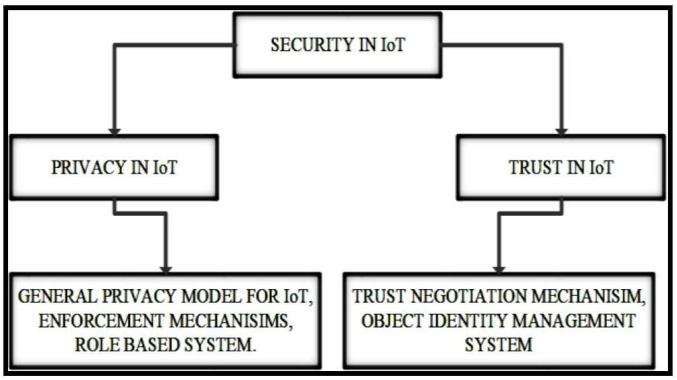

Figure 3: Dependency of Privacy and Trust on Security

IoT SECURITY REQUIREMENTS

The three basic requirements for the internet of thing's security are namely authentication/integrity, confidentiality, and access control.IoT devices must establish authentication, non-repudiation, integrity at several levels. Which is used to help devices to communication between the users and built the trust among each other .Confidentiality is important for IoT in a way that the wireless communication between one object to other different objects is particularly sensitive and vulnerable to confidentiality threats. Attackers are always snooping for confidential data and information for their use. Message or data may easily get intercepted by the adversaries for the transmitting medium.It discusses the permission in the usage of resources and data assigned

to different devices of the wide and vast area of the IoT networks. Data holder and data collector are present when dealing with access control in IoT. All the information need to be placed according to the instruction given by data holders. Data collector must collect the specific and targeted data so that the process of authentication and identification of genuine data holder can be performed.

WAYS FOR SECURITY, PRIVACY, AND TRUST IN IoT

Some of the IoT core technologies include radio frequency identification (RFID), near field communication (NFC), wireless sensor networks (WSN) . Automated information in the internet of things exchanges between 2 devices or 2 ends takes place through some communication technologies which are described below.Near field communication (NFC) is a type of contactless communication which is considered to be the important technology for IoT. As the name says, this technology is only usable when devices need to exchange their data within a short distance.Wireless sensor networks (WSNs) play important functions in the internet of things. Wireless sensors networks are the arrangements of independent nodes whose wireless interaction and communication takes place over restricted or having limitation in the place and bandwidth. A typical WSN consists of microcontroller, sensor, memory, transceiver and a power supply or battery. Radio frequency identification(RFID) is one of the essential factors in the IoT and its applications. It is a major innovation in embedded transmission and communication criterion or paradigm which allows the design of microchips for wireless communications. RFID helps to do the identification by using a unique id or a barcode in an automated way.

IOT PROTOCOLS RELATED TO SECURITY

IoT covers a large range of applications, products, and technologies. For this reason, numbers of protocolsrelated to the security for IoT are getting increased. A comparison on some of the most important protocols working at different layers in IoT can be seen in fig 4.

Layer	Protocol	Security Protocol	Inter-operability	Manage-ability	Security
Application	CoAP, MQTT	User-defined	Yes	Yes	Yes
Transport	UDP	DTLS	Yes	Yes	Yes
Network	IPv6, RPL	IPsec, RPL security	Yes	-	Yes
6LoWPAN	6LoWPAN	None	-	Yes	Yes
Data-Link	IEEE 802.15.4	802.15.4 security	Yes	-	-

Figure 4: The stack of protocol related security

ISSUES AND CHALLENGES

0.1 A. Privacy issues in the Internet of things:

Many devices are connected together, working together in both public and in private domain. There is a tinny or small difference among security and privacy, mostly security avoid to exchange and process personal information. Security constraints are mainly confidentiality, authentication, and integrity but privacy typically define as verifiability, transparency, and right purpose. Privacy is important to identify the authorized end user, user privacy, access control, to do secure communications, resilience to attacks, and the most important to build the trust level between the device or application and the end user.

0.2 B. Trust issues in the Internet of things:

Trust is developed when there are security and privacy in the object or entity. Trust is a very multifaceted concept that is influenced by many measurable and non-measurable belongings or parameters. It is associated to security and user safety in different facets of the entity, trust covers a big area as compare to security and privacy thus it is not as much as easy to build and accomplished the trust factor.

0.3 C. Issues regarding security in the Internet of things:

Area of Issues	Solutions
Authentication	Handshaking of algorithms and pre-shared keys for low power availability. RFID plays the main part in the recognition and identification of entities.
Identification	Considering their physical address and by the use of IPv6
Data management	Databases software (e.g. SQL, SQL lite etc.)
Heterogeneity	Architecture known as IDRA must be used which is particularly intended to participate in all the devices. IDRA can attach objects directly without any gateway. It covers backward compatibility and requests fewer properties.

Figure 5: Area of Issues and their Solutions

CONCLUSION

As we have discussed in this paper about the security, privacy, and trust that what is security, trust, privacy, importance, needs, issues, and challenges. IoT is an emerging technology rapidly gaining importance from last decade we have to know about the major and basic concepts of internet of things in order to perform and use the technology in our daily routines, IoT is not only used in a specific zone but it is used and applied on multiple zones either it is homes, grid, health care, industry, agriculture, and other entities because of that we have to know about the IoT and the important aspects of it, the concept of IoT is to play safe and secure by ensuring about the privacy from which the trust built and the technology can get more useable and advance in the future as the needs increases once the trust, privacy and security factor builds.

- `https://ieec.neduet.edu.pk/2019/Papers_IEEC_2019/IEEC_2019_37.pdf`