Proceedings of the Fifth International Conference on Communication and Electronics Systems (ICCES 2020)
IEEE Conference Record # 48766; IEEE Xplore ISBN: 978-1-7281-5371-1

A Survey of Privacy Leakage and Security Vulnerabilities in the Internet of Things

Amit Kumar Tyagi [0000-0003-2657-8700]
School of Computer Science and Engineering
Vellore Institute of Technology, Chennai Campus, Chennai, 600127, Tamilnadu, India.
amitkrtyagi025@gmail.com

Deepti Goyal
Department of Computer Science and Engineering,
Lingaya's Vidyapeeth, Faridabad - 121002,
Haryana, India
deeptigoyal1994@gmail.com

Abstract. In this world, where everything around use is linked with technology, be it smart homes, smart cities, smart cars, etc. Internet of Things (IoT) or Internet Connected Things (ICT) are connected todays everywhere, with everywhere which is used to build a smart environment (with physical world).

In fact, these internet linked gadgets have made our lives extremely easy, secure, and quick. But, using such devices in our daily life, people are very much concern about "their personal information". So a question raised here: "Is it (personal information) safe with these (such) devices"? When these devices are connected together, they build an ecosystem together for human being/for various applications. A lot of data is being captured and transformed into valuable forms, which is used in future for increase productivity by forms/ organisation (in many application areas), ranging from automated home appliances, smart grids and high-resolution assets, to product management. This captured and collected data creates several issues, so it requires new/ useful strategies of enhancing the present status of IoT by incorporating (or overcoming) security and privacy into its current design, structure and implementation. Hence, this article explains such issues (in IoT) like privacy breaches, security vulnerability etc., in clear manner.

Keywords – Internet of Things (IoTs), Internet Connected Things, Privacy, Security, Cyber- Attacks, and Internet of Thing's Applications.

I. Introduction

In the previous years, a number of security threats were existent in IoT and Cyber Physical Systems including those of robotics, electronic power grids, smart transportation systems, etc. The phrase 'Internet of Things (IoTs)' was first invented in the mid-1990s by Kevin Ashton, the co-founder and executive director of MIT's Auto-ID lab [1]. Significant attributes occur across a variety of meanings, including sensors, stuff, persons, operation, automation, info, network, communication, convergence, and intelligence. The Internet of Things (or Internet Connected Things or Smart Things) may therefore be described as "Intelligent interactivity between human beings and objects to share information and knowledge in order to generate new value". Billions and billions of devices are getting connected to the internet everyday as hardware is getting cheaper and smaller to fit into even the tiniest object. Manufacturers are connecting even the mundane kitchen gadgets to the internet to do some little work. Over a period of time, it is possible to turn the dumbest thing into a smart device. For example, a washing machine manufacturer collecting data to understand the product's wear and tear to build a better version in future (i.e., for future customers). However, a customer is always unaware from this kind of strategy of manufactures. So, in future a device to be unexpectedly smart. This scenario is the outcome of industries who are just thinking ways to make a device IoT enabled rather than thinking whether they should make a device IoT enabled or not. Interestingly it is not the consumer but the manufacturer who is benefitting by collecting data. Every manufacturer's primarily intention is to digitalize things to collect data. Manufacturer first aim is to attract many customers (with putting security risks at side), to make maximum profits and to stand in competitive market. Also, the customers wanted themselves to be updated with the latest technological innovations and are ignoring the associated security risks. A lot of data (called Big Data) is being generated by internet of Things (internet) and its integration. Also, this generated data is being collected on a cloud. On another side, cloud is the backbone for the Internet of Things, resources can be shared anywhere, anytime. As IoT devices or this technology evolves, human being become more familiar with smart things/ these devices. So, these internet connected/ IoT devices are used for solving some real world's problems/ tasks related to real-time scenarios like self-driving cars or health care, etc.

IoT offers a number of benefits to its clients and has the capability to modify the techniques through which the user can communicate with technology. In near future, the Internet of Things is being integrating with virtual world with physical world (together), which is difficult to protect. When it comes to security and privacy, the expected usage of sensors and gadgets in personal spaces do pose issues and problems. As physical objects are increasing in our daily life (according to our needs), then in future, detection and sharing of observations about us (by devices) will be increased automatically, i.e., require to protect our privacy. The IoT has the ability to link as many "stuff" as 10X (28 billion) to the Web by 2020, spanning from bracelets to vehicles (in the immediate future). Notice that the Internet of Things (IoT) arose as the third phase of Internet growth, the Internet phase of the 1990s was the first, whereas the web wave of the 2000s was the second [2]. With decreasing prices/ cost of sensors, processing power and bandwidth to connect devices are enabling ubiquitous connections right now. Pervasive computing follows 6A's, authorized access to anytime-anywhere-any device-any network-any-data. Internet of Things (IoTs) makes a smart environment in integration of together [3], in this smart environment several smart things works together smartly, security, and efficiently. In the development of the Internet of Things (IoT) devices/ smart things, several issues like security, privacy, scalability, lack of standards, etc., (already) has been raised. Loopholes in security (badly configured devices) may

Authorized licensed use limited to: University of Massachusetts Amherst. Downloaded on July 16,2020 at 10:14:07 UTC from IEEE Xplore. Restrictions apply.

provide a backdoor to unknown/ malicious users/hackers. Internet of Things devices are becoming more attractive to human beings (now days) than any other technologies (e.g., mobile phones), which access user's most sensitive information/ personal data, i.e., social security numbers and banking information. This is an essential issue overcome/ to received attention from research community.

A. Component of Internet of Things

Featuring IoT by sampling the numerous linked/networked devices is indeed a method to oversimplify the issue and must realize that IoT is a sophisticated environment which consists of nearly all the aspects of the Internet including analytics, the cloud, application, security and much more. Technically speaking, networked devices/gadgets linked with the internet mainly made use of three major substituents i.e., physical devices embedded with sensors, connection and architecture, and analyses and implementations. The following enabling technologies with Internet of Things are included as:

- Radio-Frequency IDentification (RFID): They aid in automatically identifying anything they are connected to functioning as an electronic barcode.
- Wireless Sensor Networks (WSN): A sensor network composed of a large number of smart sensors, allowing valuable information to be gathered, stored, evaluated, and disseminated in a variety of environments. The components that make up the WSN monitoring network include: hardware from WSN, communication stack from WSN, aggregation from Middleware and Protected Data.
- Addressing Schemes: Internet Protocol version 6 (IPv6) is used for identifying the IoT devices uniquely as it is a key aspect for controlling and monitoring the devices.
- Data Storage and analytics: Billions and Billions of IoT devices are producing continuous streams of data. In order to process the data collected and gain knowledge require AI based machine learning algorithms. These algorithms need to be interoperable and adaptive.
- Visualization: Visualization is the key to the success of any IoT application. Visualization techniques help the end users in making quick decisions.

IoT devices ae further segregated into two classes, i.e., Physical objects (like camera, smart phones, UAVs, etc.) and Virtual objects (like e-tickets, e-nook, e-wallet, etc.). In simple terms, IoT is a combination of embedded technologies including wired and wireless communication sensors and actuator device and physical objects connected to the internet. An IoT system has four major constituents: a). Sensors that collect data from smart devices b). Input which activates the sensors c). Data analysis that is performed to extract useful information. d). A monitoring system for ensuring security and privacy of the information.

Hence, this section discusses about several things likes introduction and essential components of IoTs. Further, the organization of this paper is discussed as: Section 2 discusses a vision for future, i.e., how near future can be changed/ will be with Internet of Things and Machine Learning or intelligence together. Further, section 3 discusses about some current trends in IoTs technologies. Then several Threats to Internet of Things Ecosystem like human and cyber-attacks (also some vision of IoTs in future) are being discussed in section 4. Further, will secure an IoT ecosystem using some preventive and cryptographic mechanisms in section 5. Then, security and Privacy Goals with internet of Thing's Devices (via a 360^0 view) have been discussed in section 6. Before conclusion, some challenges in IoTs devices/ with internet connected things have been discussed in section 7. In last, this work is concluded with some future work (scope) in section 8. Note that in this work, used terms 'Internet of Things' with 'Internet Connected Things' or 'Smart Things' interchangeably.

II. How Internet of Things is affecting User's Privacy?

Generally, Internet of Things enabled devices are physical gadgets with built-in Internet connectivity that allow data transmission [10]. But, a user is unaware what is happening in the background, i.e., a user have no indication that anything is happening in back-send. Are these devices are supporting users in a positive ways or in negative ways? For example, a movie named "Spy in the sky" was released in 2015.In this movie, user's location or movement was getting traced by drones (in form of/ like a bird). Such incidents are possible in real-world also. As another example, a hacker or antivirus companies have added some patches with their antivirus update, to get end-user activities. Even hackers can send malicious files to an end user which may control end user's systems/devices entirely. As discussed above, increases in connected devices/ IoTs are the main causes in generating a lot of data. Also using devices by several people without knowing such technology/ device or having low security in respective devices are the main reason of losing their footprints to other users/ attacker/ hacker. IoTs are much helpful in building Cyber physical systems, but providing automation to machines or every work may harm to society/people via tracing their movements (or footprints). These are is no guarantee that these devices will not track user's movements or reveal this collected information to other user/ outside world. Internet of Things device are being used in several applications like industries/ industrial intent, personal medical devices, smart home, wearable, smart city, smart grid, connected car, smart retail, smart supply chain, smart farming, etc. [2]. Apart that, today's IoT devices are resilience to several attacks like TREsPASS attack, Distributed-Denial-of-Service, Falsification attack, Man-in-Middle attack. Hence, with such attacks, hacker/ attacker breach or track or interfere into user's personal life/ daily life. In summary, a user may be traced in public places by several devices or by his own devices (like smart phone, laptops, or nay internet connected devise, etc.). Also, he/ she can be traced by hackers/ machines/ robots (i.e., a cyber-physical system) in his/ her home. A robot can look to his owner, i.e., at what time which work he/ she is doing and so on. According to that, machine/ robot may use this information/ traces/ patterns against his owner (in future) only. For example, in a movie named "Edward Snowden" which was made on true incident. In respective movie, Central Intelligence Agency (CIA) looks into its citizen's life and traces every movement of its citizens. Together this, CIA read all messages through mails, phones, etc., of its citizens (also put surveillance on its citizens). Hence, there was no privacy protection mechanism, even companies made to bind to share their user's data with the respective government. As another example, in China (now a day) mobile companies have to share its user's data with respective governments (as a mandatory rule). Such examples are complete violation of personal privacy. Basically, a user's privacy need to be protected and kept preserved, because

Authorized licensed use limited to: University of Massachusetts Amherst. Downloaded on July 16,2020 at 10:14:07 UTC from IEEE Xplore. Restrictions apply.

privacy a fundamental right for citizens of a country (e.g., India, USA, etc.).

Hence, major security issues in IoTs/ Internet Connected Devices are: handling data encryption, data authentication, IoT hardware issues, hardware testing (as inevitable), and managing updates (in devices). Also, major trust issues in IoT are: lack of security, leaking of privacy/ tracking footprints of users, safety (smart locks, etc.). To overcome such raised issues in IoTs and need to fulfil some goals with respect to privacy and trust. Primary security goals in IoT are confidentiality, integrity, authentication and authorization, availability, accountability, auditing, non-repudiation. On the other hand, privacy goals in IoTs are: privacy in devices, privacy during communication, privacy in storage, privacy in processing, identity privacy and location privacy and building trust with respect to respective service provider (who own IoTs devices). Hence, this section discusses about how internet connected devices may affect user's privacy in a crowd places and non-crowded places. Now how IoTs can be useful to a human being can be discussed via two scenarios (see figure 1). Here, neededto discuss one day of a user with two different scenarios [4, 5], in that intelligence or machine learning are much helpful/ in helping them to get ready for next day (for job/ work). Hence, what noticed from the discussed scenarios (discussed in [4]]) and learned here, differences among life living with and without intelligence, and importance of Machine Learning or intelligence/ artificial intelligence in near future. For new users, no matter when a user gets up, shower and coffee are being ready without ever-getting the chance to waste water or warm or cold using intelligence with (in) IoTs devices. Smart things keep/ perform event in flow/ in manner (see figure 1). Above all tasks which were done by user only (in scenario 1), can be done in sequential or in parallelized way with Intelligence. But, depending more on technology also creates several problems like leaking of privacy/ personal information, storing information without user's permission, trust, safety, etc.

Figure 1: Flow of Events with Internet of Things and new Technology like Machine Learning, or Deep Learning [4]

Hence, this section discusses about internet connected things, i.e., how they (IoTs) are changing human's being life or making their life better. Later, this section also discusses uses of IoTs (with intelligence or machine learning) in human's being life with an example (i.e., with two scenario). Now next section will discuss about the technologies which are trending now and in near future.

III. Technologies Trending Now and in Near Future

As discussed above, most of the benefits (from cloud based IoTs) are coming with huge risks, like losing of privacy loss and security breaches. To secure the IoT devices (also to preserve privacy of user in IoTs), several novel ideas/ proposed work have been proposed by many researchers [6]. The Internet is the main backbone for making a communication among devices/ machines, also a platform to reveal people's information to malicious users/ hackers. In 1990, internet/ worldwide web (a method of publishing information on the Internet) created by Tim Berners-Lee [7, 8]. Today's Internet users are in billions, it is being in maximum devices (i.e., interlinked human and creates new generations of interactive experiences). Within a few years, Internet will be the prime complement to plethora of IoT integrated environments (a whole new world filled with interlinked smart gadgets which are combined with sensors, connected to the Internet, all exchanging data and details among each other without mundane interference). It is because today Internet has a lot of information (due to having a large network of information). In simple terms, Internet became a bigger platform/ source of information (also it is due to large number of websites available on it).

Value Propositions: Internet connected gadgets being the tech-giants among modern day individuals have been linked to four major components which include Big Data, Cloud, Social Media, and mobile devices [4]. Interaction of these components (together) will fuel and shape the IoT to a new level. The 'Internet of Things' generate a lot of data (called as 'Big Data'), which is used by data scientists, researchers or organisations (or manufacturer) to do prediction/ make some decision for future. The volume of data attributable to the 'Internet of Things' is substantial. As sensors (embedded in IoTs) interact with the other things (or devices), 'Things' such as RFID tags generates huge and huge of data. In result, traditional tools fail to handle this large amount of data. Digital computation has turned out to be necessity with flexible viability. The significance of data related to IoT is contrasted with typical transaction processes and it's to be noted that these sensors are capable of capturing data meticulously. The variety of data is generated by 'Internet of Things' is also increasing/ changing frequently (due to using different types of sensors in different applications). Data (from IoT systems) authenticity has been refined due to the increased quality of the sensor while rest of the system enhances with time and experience. Consider the case of Radio Frequency Identification (RFID) tags. These tags create highly validated and authentic information from the past decade or so. Such massive amount of data, integrated with rapidly rising data significance, combined with larger variations in data elucidates the urge of Internet of Things to produce Big Data. Therefore, a complete outlook of IoT devices can be observed from the below mentioned implementations:

- IoTs for manufacturing
- IoTs for retail
- IoTs for electronics
- IoTs for automotive
- IoTs for energy and utilities
- IoTs for insurance
- IoTs for industrial
- IoTs for aviation

Above discussed point and uses of IoTs in several applications has been discussed in [3]. Hence, this section discusses trending technology of Internet of Things (IoTs) in several applications. Now, next section will discuss several raised threats in an IoT ecosystem.

IV. Potential Threat to Internet of Things Ecosystem

As discussed in [1, 4], 'Internet of Things' Generates 'Big Data'. The above discussed points are four pillars (of technology) and they're interlinked with one another and work effectively (from the aspects of cost and accessibility of records/database). However,

Authorized licensed use limited to: University of Massachusetts Amherst. Downloaded on July 16,2020 at 10:14:07 UTC from IEEE Xplore. Restrictions apply.

IoTs have a completely different prospect for these pillars, i.e. tracking and distributing personal details to malicious users (e.g. in a Hollywood movie "Eagle Eye," released in 2008, in which computer systems or army personnel track a user or their location everywhere with the help of a small drone) [4]. With increasing number of gadgets entering the IoT family, researchers have performed many privacy tests to identify the threats to IoT and to create awareness. The key threat vectors, discussed in [11], also including here:

a) Threat Posed by Compromised Devices: IoT devices contain information and the attacker have the potential target to exploit that information, for example, User fixes a security camera, it may show personal information about the user. This information can be hacked easily and the attacker can control and manage it [4, 11].

b) Threat over Communication Link: An interlinked set of IoT devices sends and receives large volumes of data, during which numerous potential threats and attacks are possible. This transmission can be interrupted, seized or manipulated during transmission. For example, an attacker can always track the footprints of a client with the help of his/her conversational details. Further, attacker can also track the energy usage of the user so as to execute an attack which would destroy the complete smart system. Here, successful threats would affect the privacy and trust existing between the user, the gadgets, the companies, etc. pertaining to the data transmitted in the IoT framework.

c) Threat on the Master: The threat (here) is on the producer and Cloud Service Provider (CSP) giving rise to problems like safety, trust and privacy. Both the manufacturers and IoT cloud possess trillions of data in quantity which prove to be extremely volatile and are a structured asset as it's determined by analytics. It's also to be noticed that this has greater competitive details with respect to APT (Asia-Pacific Tele-community) group, if leaked/ intercepted. If the master is negotiated with, it offers an opportunity to the intruders to modify and alter numerous devices simultaneously, few of which are likely to have been implemented in the field already.

In addition to all the advantages of the IoT program, many protection risks are found in IoTs and addressed in [4, 11]. Remember that internet connected devices or machines are extremely valuable for cyber attackers for several purposes:

i. Most Internet Networking (IoT) machines run unattended by humans and it is convenient for an intruder to reach them physically.
ii. A majority of the IoT components converse with each other using wireless networks such that the intruder could obtain even the intimate details by eavesdropping.
iii. Also, many of these components don't support sophisticated safety plans due to the reduced power and processing resource capabilities.

a. Human Threats

Malevolent human behaviour may be a significant challenge to your machine, for example, a disgruntled employee can attempt to exploit or kill data [12]. Human is constantly trying to find new ways to annoy, steal, and harm. Human threats can be classified as mentioned below:

- Unordered threats and issues which contain a majority of inexperienced users who avail the easily accessible hacking tools.
- Ordered and sequenced threats, create and make use of codes and contents, i.e., Advanced Persistent Threats (APT) [13]. APT is an intensive network attack which aims at highly important details pertaining to business and other institutions, in order to breach data [14].

Hence due to weaknesses in security vulnerabilities or Rogue security software, malicious users can enter in another user's system and can steal their data.

b. Common Cyber-Attacks

Using malicious code, i.e., in form of worms, virus, etc., Cyber-attacks are being done to harm users or their data (which is a cybercrime due to stealing of information and identity theft of users). In general terms, any effort to reveal, modify, kill, ruin, rob or obtain unauthorized access to or allow unauthorized use of an object is a cyber-assault assault. [15]. Generally, cyber-attacks are socially or politically motivated on internet-connected systems/ things, i.e., stealing, altering, or damaging someone information on an internet connected system/ things. Today's several attacks have been performed or formed one thing/ computer (system) to another things/ computer (systems). Many attacks on these things (internet connected devices) have been detected in the past decade. Some of these Cyber-Attacks on IoTs are listed here as:

1. Physical attacks**:** It is the subset of physical threats. Attack means that there is some attacker and his intention to do attack and tempers with hardware components. Usually, most systems run in urban settings that are particularly susceptible to physical assaults.
2. Reconnaissance attacks: It involves the illegal discovery and tracking of systems, work, or threats, fore example, analysing the network ports [16], packet sniffers [17]. Traffic jam analysis, and forwarding queries and other concerns related to IP address.
3. Denial-of-Service (DoS): A Denial of Service (DoS) attack happens as a device normally makes a computer or network resource inaccessible for its expected users. In this attack, the intruder (hacker) sends unnecessary messages demanding authentication of requests with invalid return addresses.
4. Access attacks: The attacker wants to gain to a system network, where the intruder has to find out the vulnerabilities or weaknesses in the network authentication, i.e., FTP and web services. This attack is of two types: Physical access and Remote access.
5. Attacks on Privacy: Securing privacy in IoT turns out to be a herculean task which is easily accessible due to remote access algorithms and techniques. The most common attacks on user privacy are:
    - Data mining: The attacker can extract useful information and patterns from data in large databases.
    - Cyber espionage: The attacker use malicious software and cracking techniques to steal the secret information of the individuals, organizations or the government.

Authorized licensed use limited to: University of Massachusetts Amherst. Downloaded on July 16,2020 at 10:14:07 UTC from IEEE Xplore. Restrictions apply.

- Eavesdropping: listening to a conversation between two parties [20].
- Tracking: The attacker can track the movements of the user with the help of devices Unique Identification Number (UID), for example, mobile number.
- Password-based attacks: Intruders try to recreate an authentic password which is done in two different ways: i) dictionary attack- figuring out all the plausible combination of letters and number to guess the password ii) brute force attack – taking the aid of cracking tools to find out the possible combination of passwords and to figure out the valid one.

6. Cyber-crimes: The Web and smart devices are used to misuse consumers and data for materialistic benefit, including stealing of intellectual property, identity theft, image infringement and fraud [18, 19, and 21].
7. Destructive attacks: large scale chaos and devastation often take place at the space. Terrorism and acts of vengeance are some examples.
8. Supervisory Control and Data Acquisition (SCADA) Attacks: Just like any other TCP/IP structures, SCADA [22] is also susceptible to a number of Cyber attacks [23, 24]. Attackers can exploit the systems in the following manner: i) Making use of denial-of-service to switch off the system. ii) Making use of malwares like Trojans or other viruses to take control over the system. For example, Stuxnet was the malicious virus launched on the Iranian nuclear reactor in Natanz (in 2008) [25].

Some other cyber-attacks are: Phishing. Man-in-the-middle attack, Denial-of-service attack, SQL injection, Zero-day exploit, etc and need to remember here that as the number of IoT devices are integrating together and becoming a reality to user's life, and then obviously several security threats also will be occurred. Everyday unfortunately, IoT devices are getting new attacks (with new mechanisms, code).

c. Vision of the Internet of Things

As discussed IoTs are being used everywhere now days. Also several threats have been mitigated on IoTs devices. So, a manufacturer (of these devices) needs to build these devices in future with considering issues like privacy, safety, and quality of life (for other user/ firm, which will use it in a distributed multi-user system with internet). Internet of Things is being look at outer world in the following way

a) Large Scale Ubiquitous and Pervasive Connectivity: Today's in vision of the IoT, these devices are using in creating smart environments, i.e., to makes energy, transport, cities, etc., more intelligent [29]. Integration of IoTs makes an environment which provides efficient services to users anytime, anyplace (using optimal path). IoTs in near future will be used in several areas like businesses and industrial Internet (with creating an open, global network of people, data, and things).

b) Context-Aware Computing: This needs the most in the Internet of Things, i.e. consumers need to be conscious of the computational elements (to maximize their performance and to enable automation of services). Therefore, developing intelligent worlds, content, and business apps (which support users) will entail the collection, review, and understanding of essential user background knowledge.

c) Seamless Connectivity and Interoperability: Internet Connected Things or IoT requires seamless connectivity and Interoperability, so that context information can be shared among heterogeneous devices.

d) Network Neutrality: Network neutrality (a cornerstone of the IoT vision) notes that "no information should be granted preference over another detail." The idea of linking some system to other devices at any time from everywhere therefore allows the most efficient physical route in a network / communication between the sender and the recipient.

Hence, this section discusses about several threats notified in the IoT ecosystem. Also, this section discusses about human and cyber-attacks (including vision of IoTs things) in detail. Now, next section will discuss some mechanism to secure an IoTs ecosystem in detail.

V. Securing Internet Connecting Things Ecosystem

IoT will be a game changer for the applications and business but it will raise issues like security and privacy on a large scale and requires attention from manufacturer. Usually, safety and security norms of IoT depends on the efficiency to spot and detect devices and gadgets which safeguard IoT hosting platforms and data which are then shared with numerous trusted IoT gadgets (a trusted device is loyally detectable and is linked with the provider). Passing on information with the trusted objects would further enhance the trust among users and on technical developments. Now, here discussing all necessary tasks/ components to require/ secure an IoT ecosystem.

a. Maintaining Data Integrity with Internet of Things/ Internet Connected Things

Internet of Things promises to open up new opportunities for businesses to offer exciting services. These days' insurance providers are installing IoT apps in the cars to gather customer safety data and driving information and enable insurance claims decisions. To prevent the data from the malicious user, the data should be encrypted at network layer. The principle of Blockchain (firstly used in Bit coin: the modern form of crypto currency [30], in 2009) is often used to complete this task, i.e., can offer higher safety to a dispatched and distributed system.

b. Establishing Trusted Identity Internet of Things

As discussed earlier, IoT has laid its foundation on a framework of distinctly detectable gadgets and devices, while, pubic key encryption plays a major role in developing trusteed identities. Public key cryptography has made use of the technique which involves two variant keys to exchange information amidst users/systems. One of the keys are public while the other is private. Information can be accessed and read only if both the keys are implemented right on an encrypted data. This is done with Certification Authority (CA). Further, trust is established by creating blocks and maintaining the encoded data in blocks with consistent data with respect to the preceding and the succeeding block's records.

Authorized licensed use limited to: University of Massachusetts Amherst. Downloaded on July 16,2020 at 10:14:07 UTC from IEEE Xplore. Restrictions apply.

c. Establishing a Public Key Infrastructure for Internet of Things

As seen above, identity architecture is created on a combination of public and private keys. If the private key is not safe enough then the integrity of the key is often lost. The safe creation and maintenance of these keys are of prime importance. Public keys must be secured from tamper-resistant software / encrypted data by a new workaround (which is successfully implemented along with real-time attacks). The function will easily eliminate a network attacker / attack.

d. Protecting Aggregated Big Data with Encryption

The data gathered, sent and maintained in clouds/IoT can be safeguarded with encryption methodologies. Blockchain techniques are used to secure the data, i.e., securing the data in the blocks and connect them to the succeeding blocks. Data is present in two forms - static data and dynamic data.

- Protection of Data at Rest: Each time the devices interact, a lot of data is generated which is stored at numerous locations with secure methods and techniques. Encrypting data and storing them at the server offers scalability, cost efficient storage, and quicker computation. These encoding mechanisms offer availability, veracity and accessibility of the collected data (i.e., accessible to users all the time). Storing data in a safe and secure manner and evading thee plausible entry points to harmful intruders is an issue of prime importance. To tackle this problem, institutions need to implement efficient encoding techniques with Big Data clusters. This requires flexible and autonomous file-system level encryption which can protect complicated data on the dispatched nodes.
- Protection of Data in Motion: Encryption of information poses a significant challenge as it possesses a variation increasing at rapid rates. When data moves between locations, it's often exposed to malicious attacks like fibre-tapping attack, man in the middle attack, etc. Note that an attacker can overhear the conversations/interactions by attaching cables without being identified by any other device. In this case, attackers can capture all the activities which participates in a network, which is then stolen without the owner's knowledge. In the worst-case scenario, these attacks often tamper the data and can override the controls on the full system. It's to be highlighted that encryption is mandatory at the back-end for cloud service providers, manufacturers, etc.

Data can further be secured with the help of Blockchain. Security can be offered to different data types by creation of blocks and maintaining encoded data/information with the help of consistent information when compared to the preceding and succeeding block records. This process isn't a compromised by any attack. Note that Physical protection is actually more of a concern, because such machines are typically out in the open in remote areas where anyone can access them physically. The security issues escalate significantly if anyone has physical access to the computer. This research therefore provides many ideas or strategies for protecting an IoT or cloud-based IoT network (providing security). Now, next section will discuss several security and privacy required in IoTs (via 360^0 view).

VI. Security and Privacy Goals with internet of Thing's Devices (via a 360^0 view)

In above discussion (in section 5), storing or learning patterns of user's daily activities is ok, but it is critical when it is shared with unknown device/ users. It is a major and essential challenge (issue) to overcome. Privacy is a fundamental right, which needs to be protected. It can be protected with complete isolation from outside world/ Internet-world. A user starts to interact with other devices/ people; he/she starts sharing/ is willing to share information about itself with others. Hence, some privacy goals in IoT based Cloud are included as:

- Privacy in devices: It depends on physical and commutation protection. Personal/ Sensitive information may be transmitted to other applications from a device (e.g., in cases of data theft or loss and resistance to side channel attacks).
- Privacy during communication: It is dependent on the accessibility, integrity and trust of the gadget. IoT devices must interact at the time of need, to derogate and disclose the data privacy during their interaction.
- Privacy in storage: It is to protect the privacy of data stored in devices by taking into account the following: manageable amount of data must only be maintained in the devices and regulation is to be expanded for offering safety and privacy of the user's data.
- Privacy in processing: This is completely dependant on communication integrity [26]. Information is to be stored from third parties without acknowledging the data owners.
- Identity privacy: It's the uniqueness of any gadget and can be spotted by valid entities alone.
- Location Privacy: The geographical position of relevant device should only be discovered by authorized entity (human/device) [27, 28].
- A user consists data, information, identity, location and genomic types of privacy in communication of/ with internet of things. Such types of privacy contain valuable and sensitive information, which require protection against malicious users. Similarly, some security protection required with IoTs as:
- Security of IoT devices: Security of IoT ecosystem need to be provided physically. When an IoT ecosystem is being like smart grid, then from require some manpower/ human being to take care that site, i.e., protection site against any kind of damages. For example, organisations are hiring persons for taking care of their infrastructure (i.e., in telecom industry).
- Security in IoT devices: Proper encryption mechanism, efficient algorithms to collect data in a database, access control to known users, etc., are some essential components need to include when IoTs devices is being used.

Hence, this section discusses several security and privacy goals with respect to internet connected things via 360^0 view. In this, found that privacy of information stored/ communicated in devices should be persevered and protected, also security of devices and

Authorized licensed use limited to: University of Massachusetts Amherst. Downloaded on July 16,2020 at 10:14:07 UTC from IEEE Xplore. Restrictions apply.

enough level of security need to be provided in IoTs. Now, next section will discuss about some challenge in IoTs.

VII. Issues and Challenges in Internet Connected Things

In the past decade, several challenges have been investigated in IoTs and need to focus on these challenges to encourage higher growth rate of IoT (in near future), and to provide opportunities to future researchers to do their research work. Industry also can consider these challenges to capture new competencies and capacities. These challenges (investigated in an IoT ecosystem) can be discussed as:

- Infrastructure: An Infrastructure is an environment which is interoperable, trustable, mobile, distributed, valuable, and powerful for provide services to human beings. An IoT ecosystem consist several emerging applications in it, i.e., like Smarter Cities, Smart Grid, Smart Building, Smart Home, Intelligent Transport Systems, and ubiquitous healthcare, etc. Due to that, large numbers of address schemes are required to provide address to each and every connected IoTs (to offer offers scalability, flexibility, tested, extended, ubiquitous, open, and end-to-end connectivity). Note that Addressing schemes are used to identify with respect to identify sender's identification/ location, to provide security to devices.
- Data and Information: Lots of data is being generated with these devices (in integration), which is a major challenge to handle, and analysis. Modern analytic tools/ new big data solutions are required (by service providers) to analyse data, and discover relevant trends and patterns for future purpose.
- Security and Privacy: Internet Connected Devices (ICD) can communicate with consumers, transmit data back to service providers, and compile data for third parties such as researchers, health care providers, or even other consumers. Hence, issues including privacy related to personal data, and data sharing are emerging, which shows the importance of trust in an IoT ecosystem.
- Ecosystem: IoT has been evolving quite a lot. 'Things' seem to possess increased number of details linked to them, and have started to sense, interact, and create novel data. Services linked to IoT are likely fetch £200bn annually. This would further bring about innovation, and development in arenas like components, devices, wireless connectivity, system integration and decision-support tools.

A. Challenges in Internet of Things

A key challenge in machine learning is "How to interpret the Input Data and what are potential Security Threats and Device Vulnerabilities"? A lot of comprehensive research has been performed from the viewpoint of IoT protection up until now and similar work can be categorized into device security, program security, and network security. Some few problems in this regard can be included as:

a) Design of Service oriented Architecture (SoA) for IoT: SoA has to handle massive amounts of devices which are linked to the system which help organize scalability issues. Problems like data transmission, computation, and supervision becomes a challenge.

b) Heterogeneity: IoTs provide a heterogeneous, complex network structure. This, in effect, increases the confusion between specific types of devices through means of multiple networking systems revealing the network's rude actions to be dishonest, sluggish, and unstandardized. Managing linked artefacts through encouraging and managing them by interaction between systems, such as hardware components and/or software resources, after providing architectural and protocol level addressing, recognition and optimization is a significant research task.

c) Lack of Service Description Language (SDL): The absence of Service Description Language in connected services leads to development, execution and source integration a herculean task by elongating the dissemination time (due to/ causing loss in market). A Novel SDL may and change or solve several problems like product dissemination and must identify a commonly accepted SDL, so powerful service discovery methods and object naming services need to be implemented.

d) Lack of a Unified infrastructure: IoT is designed with a traditional network/ IoT makes CT environment. This environment is affected by its connection. So, require a unified information infrastructure to connect large number of IoTs devices (to produce real-time data).

e) Handling Large Data base: Today's existing/ Traditional Data Base Management System (DBMS) cannot handle the originated data, because of the huge data (generated or collected). The current fault tolerance system is in capable of managing the high-speed generated data. A new IoT based data centric architecture need to be proposed to tackle this issue.

f) Format of Data generated by IoTs: The data generated from IoTs devices (connected through internet) will be in present in different volume, variety and formation. So big data/ IoTs generated data specific design should be invented to handle these types of data.

B. Issues in Internet of Things

IoT system includes large number of nodes which should be identified uniquely in the network configuration. Since the IPv4 numbered addresses are about to exhaust, so have to find a new addressing scheme like IPv6 to configure all IoTs devices. Further, different devices use different protocols to handle hardware/ software compatibility, this is also a major issue with IoTs. Hence, the lack of standardised tools for security, communication and identification need to be solved to make the IoT system efficient, accurate and safe (privacy preserved). The universal applicability of IoT and associated technology would rely in large measure on network cum cyber security and data protection. IoT is extremely dynamic and heterogeneous in design, and is often facing serious challenges to protection and privacy. The key obstacles that hinder IoT to being damn secure are delivery, versatility and sophistication. From [4] and due to the large number of attack vector presences on IoT entities, privacy protection in the IoT environment is more vulnerable than in traditional information and communication technology (ICT) networks. For example, the IoT-based health care tracking device would gather data from patients (e.g., heart rate, heartbeat, body temperature, breathing, etc.) and

Authorized licensed use limited to: University of Massachusetts Amherst. Downloaded on July 16,2020 at 10:14:07 UTC from IEEE Xplore. Restrictions apply.

then transmit this information back to the doctor's office or hospital over the Web. When tata is transmitted over the network, there are chances of data being breached. In these cases, the life of the user is at stake and at high risk. In such cases, most of the frameworks don't consider the safety and security of the user which is one of the major drawbacks which need to be addressed. Hence, as Data is collected or produced in raw form, i.e., consist non-relevant handouts. And this generated data is too helpful in decision making in several applications. The value of this collected/ generated data is only possible after analysis/ filtering process. So efficient and modern tools to analysis this collected data needs to developed. Also, a commonly accepted service description language (which is compactable with different communication and implementation) must be identified to make the development process easier.

Hence, this section discusses several challenges in internet of things like heterogeneity, lack of unified infrastructure, lack of unified standards, huge data base, huge consumption of energy, etc. Some more work towards IoTs devices has been discussed in Table 1 (in appendix A). Hence, these issues, challenges can be considered as future work in near future from/ by respective interested researchers/ research community. Now, next section will conclude this work in brief (with some future scope of this work for future).

VIII. Conclusion and Future Scope

Today's internet of things are being used everywhere, i.e., in many applications (like smart home, smart transportation, smart farming, etc.) to make human life easier. Even some countries are insisting their citizens to use these devices, for example, in India, Amravati (new capital of Andhra Pradesh state) will be first smart city. Similarly, Dubai will work completely on smart things, i.e., as a smart city before 2022. So, as uses of these devices are increasing, attacks will also be increased in near future. This work provides a detail description of internet connected things. It also discusses some serious concerns and challenges in IoTs in near future. These investigated issues, challenges need to be overcome or require attention from research community. Also, major limitations of IoTs like Battery life extension and Lightweight Computation are also needed to be improved (for providing efficient, smart, and secure services for a longer-time). Therefore, system level security, master computer safety, encryption of information / communication ties is essential to conducting secure operations (including IoTs). In summary, instead of searching for a new tool, current methods can be developed to protect IoTs / IoT ecosystem. For the future works, must concentrate on providing the existent security controls and enhance the novel and sophisticated applications to drill the further implementation of IoT (because integration of IoTs in several applications and in many counties is growing exponentially).

References

[1] TELEFÓNICA I+D: Internet of Things + Internet of Services (2008).
[2] Simona Jankowski, et al., The Internet of Things: Making sense of the next mega-trend, Goldman Sachs Global Investment Research's report, Sptemmber 3, 2014.
[3] Amit Kumar Tyagi, Nandula Anuradha, G. Rekha, Sonam Sharma, and Sreenath Niladhuri, How a User will look at the Connection of Internet of Things Devices?: A Smarter Look of Smarter Environment, ICACSE: 2019: 2nd International Conference on Advanced Computing and Software Engineering, KNIT Sultanpur, 2019, India, 8-9 February 2019.
[4] Amit Kumar Tyagi, and M.Shamila, Spy in the Crowd: How User's Privacy is getting affected with the Integration of Internet of Thing's Devices, SUSCOM-2019: International Conference on Sustainable Computing in Science, Technology & Management (SUSCOM-2019). Amity University Rajasthan, India, 26-28 February 2019.
[5] https://towardsdatascience.com/iot-machine-learning-is-going-to-change-the-world-7c4e0cd7ac32
[6] Arbia Riahi, Sfar Enrico Natalizio,Yacine Challal, Zied Chtourou, A roadmap for security challenges in the Internet of Things, Digital Communications and Networks, Volume 4, Issue 2, April 2018, Pages 118-137.
[7] https://en.wikipedia.org/wiki/Tim_Berners-Lee
[8] https://www.w3.org/People/Berners-Lee/
[9] https://impact.com/marketing-intelligence/7-vs-big-data/
[10] https://www.optimusinfo.com/blog/understanding-the-7-vs-of-big-data
[11] Amit Kumar Tyagi, G. Rekha, and N. Sreenath, Beyond the Hype - Internet of Things Concepts, Security and Privacy Concerns, 22-23 March 2019, in Proceeding of Springer/ International Conference on Emerging Trends in Engineering, College of Engineering (ICETE), Osmania University, Hyderabad, Telangana, India.
[12] http://online-passport.info/comsecpriv/?page_id=41
[13] C. Tankard, Advanced persistent threats and how to monitor and deter them, Network security, vol. 2011, no. 8, pp. 16–19, 2011.
[14] F. Li, A. Lai, and D. Ddl, Evidence of advanced persistent threat: A case study of malware for political espionage, in Malicious and Unwanted Software (MALWARE), 2011 6th International Conference on. IEEE, 2011, pp. 102–109.
[15] American Government, Power and Purpose: Political science, Political science, book, CTI Reviews – 2016.
[16] S. Ansari, S. Rajeev, and H. Chandrashekar, Packet sniffing: a brief introduction, Potentials, IEEE, vol. 21, no. 5, pp. 17–19, 2002.
[17] M. De Vivo, E. Carrasco, G. Isern, and G. O. de Vivo, A review of port scanning techniques, ACM SIGCOMM Computer Communication Review, vol. 29, no. 2, pp. 41–48, 1999.
[18] B. Schneier, Secrets and lies: digital security in a networked world. John Wiley & Sons, 2011.
[19] J. M. Kizza, Guide to Computer Network Security. Springer, 2013.
[20] I. Naumann and G. Hogben, Privacy features of european eid card specifications, Network Security, vol. 2008, no. 8, pp. 9–13, 2008.
[21] C.Wilson, Botnets, cybercrime, and cyber-terrorism: Vulnerabilities and policy issues for congress." DTIC Document, 2008.
[22] A. Daneels and W. Salter, What is SCADA, in International Conference on Accelerator and Large Experimental Physics Control Systems, 1999, pp. 339–343.
[23] A. Nicholson, S. Webber, S. Dyer, T. Patel, and H. Janicke, Scada security in the light of cyber-warfare, Computers and Security, vol. 31, no. 4, pp. 418–436, 2012.
[24] V. M. Igure, S. A. Laughter, and R. D.Williams, Security issues in scada networks, Computers & Security, vol. 25, no. 7, pp. 498–506, 2006.
[25] M. Kelleye, Business Insider. The Stuxnet attack on Irans Nuclear Plant was Far more Dangerous Than Previously Thought, http://www.businessinsider.com/stuxnet-was-far-more-dangerous-thanprevious-thought-2013-11/,2013, [Online; accessed 03-Sep-2014].
[26] C. P. Mayer, Security and Privacy challenges in the internet of things, Electronic Communications of the EASST, vol. 17, 2009.
[27] A. R. Beresford, Location privacy in ubiquitous computing, Computer Laboratory, University of Cambridge, Tech. Rep, vol. 612, 2005.
[28] Amit Kumar Tyagi, N. Sreenath, Future Challenging Issues in Location Based Services, International Journal of Computer Applications (ISSN: 0975 –8887), Volume 114, No. 5, pp.51-56, March 2015.
[29] Misra, Sridipta, Maheswaran, Muthucumaru, Hashmi, Salman, Security Challenges and Approaches in Internet of Things,Engineering Signals & Communication, 2017 (Available at: https://www.springer.com/in/book/9783319442297#reviews).
[30] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

Authorized licensed use limited to: University of Massachusetts Amherst. Downloaded on July 16,2020 at 10:14:07 UTC from IEEE Xplore. Restrictions apply.

Appendix - A

Table 1: Challenges, Issues and Cyber-Attacks including Solutions in Internet of Things

S.No	Challenges	Issues	Cyber Attacks	Overcoming Solutions
1.	Security	As the IoT connected devices increases it will also increases the opportunity to exploit security vulnerabilities for an attacker	-	A collaborative approach to security will be needed to resolve this issue
2.	Privacy	The gathering of these details showcases legal and governing tasks which face data security and privacy norms.	-	Strategies and techniques need to be created to assure and respect individual privacy decisions spanning across a wide spectrum of choices, by embedding innovation in methods and services.
3.	Standards	Absence of standards can enable stupid behaviour by IoT devices.	-	It requires a creative architecture and normalization of computation tools, methods, and interfaces, combined with the implication of IPv6, will be essential in the future.
4.	IOT botnets aiming at cryptocurrency	The rising mining competition which is joined with the novel use of cryptocurrency proves to be ana rea of interest for hackers.	-	IoT implementations, frameworks, and interfaces which depend on Blockchain have to be governed and consistently monitored.
5.	Home Invasions	It has chances of portraying your IP address which can indicate your residential details.	Such crucial details can be sold by the hackers to malicious people.	-
6.	Remote Vehicle access	It also possesses a greater risk of a car hijack.	-	-
7.	Easy exposure	IoT devices are not resilient to third-party exposure — they either lay open or easily accessible to anyone.	This means that an intruder can either easily steal the device, connect the device to another device containing harmful data, or try to extract cryptographic secrets, modifying the programming or even replacing those devices with malicious ones in which the intruder has complete control.	-
8	Machine Phishing	-	Hackers increasingly will try to infiltrate IoT and operational networks to send false signals that in turn cause owners or plant operators to take actions that can be damaging.	-
9	Infrastructure	It requires large number of address schemes. Addressing schemes are used to identify with respect to identify sender's identification/ location, to provide security to devices.	-	-
10.	Data and Information	To handle and analyse the data generated by the devices	-	Analytic tools / new big data is required
11.	Security and Privacy	1. With IoT being in the lime-light, numerous challenges for supervisors and users are being exposed, 2. Privacy linked to personal details and data exchange.	-	-
12.	Ecosystem	It stimulate innovation and growth in areas such as components, devices, wireless connectivity, system integration and decision-support tools	-	-

Authorized licensed use limited to: University of Massachusetts Amherst. Downloaded on July 16,2020 at 10:14:07 UTC from IEEE Xplore. Restrictions apply.