




Beyond the Hype: Internet of Things Concepts, Security and Privacy Concerns

Amit Kumar Tyagi¹ , G. Rekha², and N. Sreenath³

¹ Department of Computer Science and Engineering,
Lingaya's Vidyapeeth, 121002 Faridabad, Haryana, India
amitrktyagi025@gmail.com

² Department of Computer Science and Engineering, Koneru Lakshmaiah
Education Foundation, Vaddeswaram, Guntur 522502, Andhra Pradesh, India
gillala.rekha@klh.edu.in

³ Department of Computer Science and Engineering,
Pondicherry Engineering College, Puducherry 605014, India
nsreenath@pec.edu

Abstract. Today's Internet of Things (IoT) has occupied maximum fields/areas where they are working a tremendous works, i.e., providing better life experience to human beings. For example, in e-healthcare, IoT devices are providing a lot of data to doctor, also helping doctors to identify certified medicine or discusses or helping doctors to remember various certain activities of a patients, etc. Similarly, chatting applications (online social networking) have made communication easier among human beings. IoTs are with everything (applications) in this physical world and they are connected on a large scale and integrated securely through Internet infrastructure. But, are we satisfied with this security (security in IoTs)? On another side, these devices (IoT) or applications are collecting a data from your every movement/tracking your (humans) movement. This data is stored as large data (called big data) and used or sold to third parties (like organization) to make profit for them (via analytics process). These devices have an issue of leaking your movement or person to unknown users, which is a serious issue. This work (or article) will discuss some facts like about IoTs, which may protect people or provide awareness to people or protect them when they are visiting any website/browsing or coming online (for working something or making a communication).

Keywords: Internet of Things · Security · Privacy · Big data · Privacy in virtual world

1 Introduction to Internet of Things

The Internet has evolved in 1990 (creation of World Wide Web (W3), a network of network: concept created/built by Tim Berners-Lee [1]) but has received attention from maximum customers during the past decade only. Today's Internet has become the richest source of information and utilize by multiple devices for example, for finding path, or any hotel over the road network (using help of Global Positioning System (GPS)). Internet has seen its first revolution in 1990 to 2000, and second revolution

from 2001 to 2010, whereas, third revolution since 2011 onwards to till date. Till 2010, Internet was a universe of interlinked human and creates new generations of interactive experiences, but today it has moved to a new level, i.e., provide or using (sharing) information with internet of things or smart devices. Internets of Things (IoTs) or Internet Connected Devices are the devices (with consisting sensing feature) or use Internet network for making a communication or provide better life experience to human beings. In general, IoT or smart devices are the concept of connecting smart objects or operating together to solve some specific/real – world problems. With respect to this, IoT or Internet Connected Devices has become popular since 2011, i.e., with the rapid development of small low-cost sensors, wireless communication technologies, and new Internet techniques. *Today's several applications that use IoT* devices are: intelligent transportation, communication, e-healthcare, smart home, smart animal farming, finance, retail, environmental monitoring, etc. [2]. Hence we can say that (as discussed previously) now days, we are living in the third revolution of Internet where internet is connected with IoT, “a world of networked smart devices equipped with sensors, connected to the Internet, all sharing information with each other without human intervention”. Note that “Internet of Things” term was first time coined by the cofounder and Executive Director of MIT’s Auto-ID lab, Kevin Ashton in the mid 1990s [3]. Various definitions have been given by various scientists and researchers (in the past decade), but most of the accepted definition is “Intelligent interactivity between human and things to exchange information & knowledge for new value creation” [4]. Hence, with the rise of connected devices (with internet of things) and connected individuals (systems/devices with sensor), we received combination of four terms (i.e., big data, cloud, social media, and mobile devices and things) or technologies (technology pillars) which works as fuel to industries and help IoTs to re-shape [5]. All these four pillars (of technology) (big data, cloud, social media, and mobile devices and things) are interconnected with each other and work efficiently (with respect to cost and accessing to find/search records over records or a database). But, IoTs have different views/aspects for these pillars, i.e., tracking or leaking information of user to malicious users (by malicious systems/devices, for example, in a Hollywood movie “Eagle Eye”, computer systems or army personal track a user or its location everywhere with the help of small drone) [5]. Basically, this issue (with people) is a long (complex) process/task to discuss and highly critical to taking care of/focus, so this issue is being discussed in further sections with several suggestions and technology (also refer Table 1). Apart that, discussing IoT features by providing total number of connected devices/connections makes IoT explanation easier. In general, IoT is a complex ecosystem encompassing all aspects of the Internet, including analytics, the cloud, application, security, etc. In technical words, connecting devices/things with internet used three main technology components (i.e., physical devices with sensors/connected things, connection and infrastructure, and analytics and applications) [5]. Today’s Internet of Things are providing several benefits to users/customers through several applications like smart farming, smart parking, smart homes, etc. IoT devices have the potential to change the ways of communication completely (with people and technology). In future, IoTs is likely to mix the virtual and physical worlds together to provide an easy and comfort experience to everyone (organizations or people). But, the items which will contain sensors to produce data (home, the car, and with wearables

and ingestible, even the body puts particular) will put several security and privacy challenges. Now day's physical objects are increasing with a high rate in developed countries (including developing countries) to provide growth/progress to respective nation/country. Human in these countries uses IoT devices to increasing productivity of their business (e.g., retail, e-commerce, etc.) or protect themselves (e.g., smart home), etc. These increasingly internet connected devices detect and share each and every observations about us, and store this information in the respective database/server (to which these devices are interconnected). But, note that here these devices comes with a critical issue, i.e., 'privacy'. All users require/want privacy all the time or want to protect their personal information from outside world/unknown user/strangers.

Now days Internet of Things (IoTs) devices are using much in our (human-being) lives/real-world's applications than mobile phones, but both devices contain our personal data like contacts, messages, social security numbers and banking information, even every activity made by us online (being made on internet or made by devices) or offline. It also accesses records which are running offline to our Systems/Mobile/Devices (in the backend). Also, various security concerns can be with respect to a single device, for example, a mobile phone can quickly turn to 50 or 60 concerns [6] when considering multiple IoT devices in an interconnected home or business (e.g., cost, time, security, privacy, etc.). Importantly, we need to find that which/what IoT devices have access to (i.e., need to understand their security risk). Note that the growth in IoTs/connected devices has increased since the last decade. With this, IoT also have increased the potential attack surface for hackers and other cyber criminals (e.g., Ransomware attack affect millions of computers in 2017 and steal TeraBytes of data). More devices connected online (to Internet) means more devices require protection, whereas, IoT systems are not usually designed for cyber-security. In current days, the numbers of cyber-criminals/attackers are increasing every day, and the data breaches by them is increasing every day and it will be continue in future also. Several other issues (for mobile security) are already a challenge with respect to connected devices (i.e., IoTs) and will be continued in future. For example, let 10 IoT connected devices is not creating problems for a user, but what if IoT devices are in billions a connected together, then each one represents a potential doorway into our IT infrastructure and our company or personal data. Thinks "How much data these connected devices can collect"? Note that when internet of things connects together, a lot of data will be generated, collected at several locations for making valuable decisions in future for various applications/areas like automated home appliances, defence, smart grids and high-resolution assets. Storing similar data at several locations work as backup in emergency-case. These concerns require new methods, strategies, regulations to protect IoTs ecosystem (i.e., by incorporating security and privacy into its design and implementation (refer Sect. 3 and 4)). Note that IoT ecosystem is a network of many internet connected things which are connecting together, and sharing information with each other's.

Hence the remaining part of this work is organized as: Sect. 2 investigates several threats in internet of things ecosystem. Also, this section discusses analysis of these (respective) attacks with possible solution/countermeasure. Then, some critical challenges have been included in Sect. 3. Then, this work provides many suggestions or techniques (methods) to secure an IoT ecosystem in Sect. 4. In Sect. 5, this work tells

us what we can do/solutions for avoiding tracking of IoTs or not being trapped with IoTs devices. In last, this work is concluded (in brief) with some future remarks in Sect. 6.

2 Threats with Internet of Things

The growth in IoTs/connected devices is increasing and will be increasing over the next decades. Several things/devices are connected to the Internet now days (and it will be always increasing), i.e., these (IoT) devices provide a virtual environment to human being/to a physical object, but when it get used as services with applications, this virtual form start to interact and exchange essential or important information (of respective users whoever are using these devices), and these devices make useful decisions based on this collected information/data. Now, there are several IoT threats which can be categorized into four types: Privacy, Security, Trust and Safety. In security, denial of service and other attacks are possible in IoT. In privacy, like background knowledge, timing or transition etc., attacks (with the personal information) possible done (by cyber criminals). IoT leads to several physical threats in several national projects/departments/areas, for example, automation industry (cars and homes), environment, power, water and food supply, etc. Note that when many applications interconnect with these devices to make a smart environment (with device to device or machine to machine), we need to consider security (physical), privacy (data, identity and location). Due to located or using IoT devices in sensitive areas like e-healthcare, then these devices may get tampered/accessed by the individual attacker/a group of attackers for their financial use (read or change data) [6]. With such attacks/access, attacker could control a system (which is built by integration of IoT) and change functionality of this system accordingly. For example in 2010, Stuxnet virus by spread by some attackers in Iran to control/damage their nuclear weapons. Internet of Things security is no longer a foggy future issue [6, 7], as more and more such devices enter the market and our lives, i.e., from self-parking cars to home automation systems to wearable smart devices. Now days there are (will be in future) so many sensors, so many devices, that they are even sensing you, but they are always around you to track your footprint. It is tracing your every movement/task (made by your online/offline) all the time. So, we need to be aware from such types of attacks/tracking.

2.1 These Threats Are in Real

Among the recent examples, one attacker hacked into two cars and wirelessly disabled the brakes, turned the lights off and switched the brakes full on, i.e., all beyond the control of the driver [8]. In another case, a luxury watercraft/yacht was controlled by some researchers, i.e. via hacking the GPS signal (which was embedded in watercraft for navigation-purpose). In summary, a full control can be reach to cyber attacker/third party/user to take benefits against a respective user. Also, hackers can take over automated/smart home through tampering or hacking hubs (fixed in a home), i.e. IoTs devices are being so vulnerable, which allow attackers to look into or control with heating, cooling, lighting, power and door locks, (also similar for industrial control

systems). For example, in Hollywood movie “I.T” (released in 2016), an attacker tracks every movement of a victim (from a remote location) and tries to blackmail him/her. Also in similar movie, attacker tries to control his home automation, phone or other connected devices (to internet). Through this, attacker makes pressure on victim to accept his proposal, or blackmail other person for his financial purpose. Moreover this, now days, we are already looking hacked TV sets, power meters (i.e., used to steal electric power), smart phones, video cameras and child monitors [5, 12]. Hacking such devices (i.e., internet connected devices) has raised serious privacy concerns. Today’s we can imagine a worm that would compromise large numbers of these Internet-connected devices (on a large scale) and can controlled them via a botnet [15] or a collection of computer infected system (e.g., Wannacry attack, Ransomware attack, HTTP bot, etc.). It is not just the value or power of the device that an attacker/malicious user want. An attacker wants to slow down network bandwidth through a DDoS (Distributed Denial of Service) attack. Note that here biggest issue is not security of IoT devices, but a privacy issue (collected information leaked by devices to other connecting devices) is a great concern. Also, with low bandwidth, attacker can compromise device and can use it against a user/attack a third party. Now imagine a Botnet of 100,000,000 IoT devices all making legitimate website requests on your corporate website at the same time. In result, respective website will get slow down and will not properly. With such incidents, in near future, IoT will create unique and complex cases as security and privacy challenges for several industries/organizations.

Also, machines are becoming autonomous, so they are able to interact with other machines (in near future) and are free to make decisions which may impact the physical world. For example, problems with automatic trading software, which can get trapped in a loop causing market drops. The systems may have fail safe built in, but these are coded by humans who are fallible (i.e., error-prone), especially when they are writing code that works at the speed and frequency that computer programs can operate. If a power system were hacked by some attackers and they turned off the lights of an area/a city. It is not a big issue/problems for many users, but it matters for thousands of people who are present in the subway stations (i.e., in hundreds of feet underground in pitch darkness), then this issue became too (highly) critical. Such issue really requires attention from research communities in near future. Hence, Internet-Connected Things (ICT) allows the virtual world to interact with the physical world to do things smartly and that come with several safety issues.

2.2 Some Potential Threats to Internet of Things Ecosystem

When several IoT devices are interconnected together, they create an IoT ecosystem, which work together (as automatically) to serve firms/organizations in an efficient manner. But as discussed above, these devices face several security and privacy issues. Several researchers have performed many security tests to expose IoT vulnerabilities, and make the world (or people) aware of the potential security concerns of internet connecting devices without proper security measures. Some of the key threats are included here as:

- **Threat Posed by Compromised Devices:** Since many devices contain inherent values by their design and nature of functions, a connected device presents a potential target to be exploited by an attacker. A connected security camera could expose personal information of users [4], for example, a user's location when compromised. Once these devices become trusted, then these devices are easy to hack or tamper, through this controlling, managing things become easier. It is like that controlling the lights in a house/business offices, or controlling an automobile or medical device which may affect human health/physical harms [4]. Can we put trust on these devices? If yes, then how much? This question is really a tricky one.
- **Threat over Communication Link:** This threat contains monitoring and intercepting messages during a communication session. A lot of data is being transmitted among these devices/in the IoT ecosystems (a network of connected IoT devices together), but during this transmission/transfer of information via communication, various attacks are possible, which is too dangerous and critical. Note that this communication can be intercepted, captured, or manipulated (or shared with others/unknown users) during transmission. For example, an attacker may trace the footprints of a user via his/her communication, on the other side, attacker may track energy usage (based on downtime and uptime of a system for firms/organizations/users) to plan an attack on the entire smart system/home system/industrial control systems [4]. Whereas, other attacker can manipulate the data (which is transmitted to the utility company/firms/organizations) and may affect this information. Here, successful attacks may affect trust among user, devices, firms and manufactures (of such devices) with respect to data transmitted in IoT infrastructure.
- **Threat on the Master:** Threats against manufacturer (of IoT device) and Cloud Service Providers (CSP) raises several critical issues (in IoT ecosystem) like safety, trust, privacy. As manufacturer and IoT cloud (both contain trillions amount of data, i.e., in which some data is highly sensitive data). This data is so useful, core, strategic asset because it contains some meaningful information in it (determined by analytics process [9]). Note that this has higher competitive information in view of underground APT (Asia-Pacific Tele-community) group, if leaked/intercepted. If the Master is compromised, it gives opportunity to an attacker to manipulate many devices at once, some of which may have already been deployed in the field. For example, if a provider who issues frequent firmware/software have the mechanism compromised, malicious code could be introduced to the devices.

Note that the small size and limited processing power of many connected devices could limit the use of encryption and other security measures. It may also be difficult to patch flaws in low-cost and essentially disposable IoT devices.

2.3 Analysing Different Types of Attacks (with Possible Solutions)

In general, the security attacks are categorized into four broad classes, i.e., Low-level attack (when an attacker tries to attack a network and in result fail to do attack on respective network), medium-level attack (when attacker/intruder/eavesdropper just attack on a network to listen the medium without altering any information/integrity of data), High-level attack (when an attacker tries to attack on a network and in result, it

alters the integrity of data/modifies the data) and Extremely High-level attack (when an intruder/attacker/eavesdropper attacks on a network (with unauthorized access) and performing an illegal operation, i.e., making respective network unavailable, and sending bulk messages to other users, or jamming network). Apart such attacks, the IoT is facing various types of attacks including active attacks and passive attacks [10, 11], which may easily disturb the functionality and abolish the services of communication link/network. Note that in a passive attack, an attacker just sense messages (passing through) or may steal the information, but never attacks physically (this attack is similar to medium level attack). On the other side, in active attacks case, attacker disturb the performance of a network/communication physically (this attack is similar to extremely high level attack). Note that in general, active attacks can be classified into two categories, i.e., internal attacks and external attacks [11]. Any devices can be prevented against any vulnerable attacks via using proper awareness/making communicate smartly through these devices. Hence, the security constraints must be applied to prevent devices from malicious attacks.

Different types of attack, nature/behavior of attack and threat level of attacks with possible solution have been discussed in Table 1. Hence, this section discusses several threats like Route diversion, eavesdropping, DoS, etc., investigated in IoTs with their behavior, level and possible solutions for respective attack. Now, next section will discuss several common challenges in internet of things in detail.

Table 1. Different type of attacks with possible solutions for respective attacks

Type	Threat	Behavior	Possible solution
Passive	Low	It is used to identify the information about the target node. Examples include passive eavesdropping and traffic analysis. Intruder silently monitors the communication for his own benefits without modifying the data	Ensure confidentiality of data and do not allow an attacker to fetch information using symmetric encryption techniques
Man in the middle	Low to medium	Examples of this attack include Alteration and eavesdropping. An eavesdropper can silently monitor the transmission medium and can do modification if no encryption is used and also manipulate the data	Ensure integrity by applying data confidentiality and proper integration. Encryption can also be applied to avoid data modification
Eaves-dropping	Low to medium	Causes loss of information, for example in medical environment, privacy of a patient may be leaked by sensing the transmission medium	Apply encryption technique on all the devices used in communication

(continued)

Table 1. (continued)

Type	Threat	Behavior	Possible solution
Gathering	Medium to high	Occurs when data is gathered from different wireless or wired medium. The collected message may get altered by the intruder. Examples are skimming, tampering and eavesdropping	Encryption, Identity based method and message authentication code can be applied in order to prevent the network from this type of malicious attacks
Active	High	Effects confidentiality and integrity of data. Intruder can alter the message integrity, block messages, or may re-route the messages. It could be an internal attacker	Ensure both confidentiality and integrity of data. Symmetric encryption can be applied to preserve the data confidentiality. An authentication mechanism may be applied to avoid unauthorized access
Imitation	High	It impersonate for an unauthorized access. Spoofing and cloning are the examples of this attack. In spoofing attack a malicious node impersonate any other device and launch attacks to steal data or to spread malware. Cloning, re-write or redundant data	To avoid from spoofing and cloning attacks, apply identity based authentication protocols. Can use un-clonable function as a countermeasure for cloning attack
ePrivacy	High	Intruders fetch the Sensitive information of an individual or group. Such attacks may be correlated to gathering attack or may cause an imitation attack that can further lead to exposure of privacy	Anonymous data transmission, Transmission of sample data instead of actual data can help to achieve privacy. Can also apply techniques like ring signature and blind signature
Interruption	High	Affects availability of data. This makes the network unavailable	Accessing of data and usage of data is restricted by some authorization technique
Routing diversion	High	Alter the route of transmission to create huge traffic and hence the response time increased	Apply connection oriented services to avoid route diversions
Blocking	Extremely high	It is type of DoS, jamming, or malware attacks. It create congestion in the network by sending, huge streams of data, similarly different types of viruses like Trojan horses, worms, and other programs can disturb the network	Firewall protection, apply packet filtering, anti-jamming, active jamming, and updated antivirus programs in order to protect the network from such attacks

(continued)

Table 1. (continued)

Type	Threat	Behavior	Possible solution
Fabrication	Extremely high	The authenticity of information is destroyed by injecting false data	Data authenticity can be applied to ensure that no information is changed during the data transmission
Denial of Service	Extremely high	To disturb the normal functionalities of device, the malicious node create traffic in the network by retransmitting the same data and by injecting bulk messages into the network	Cryptographic techniques help to ensure security of network. Authenticity helps to detect the malicious user and block them permanently.

3 Common Challenges in Internet of Things

As discussed above (in Sect. 3), the security, privacy, safety, etc., issues are the biggest challenge to rectify/solve in IoT ecosystem. In general, challenges are the problem where research is still going on or questions still require answers (still require attention from research communities). These issues and challenges require attention of researchers and need to be solved for providing trust in devices (through this, industry will get new competencies and capacities) and higher growth rate of IoTs devices. Some major challenges can be (identified from various areas in IoTs application/its ecosystem) included as:

- a. Infrastructure: Today's Smart Infrastructure like Smarter Cities, Smart Grid, Smart Building, Smart Home, Intelligent Transport Systems (ITS), and ubiquitous healthcare, etc. [2] require safety (need to be trustable, mobile, distributed, valuable, and powerful enabler for these applications) as an essential component in its infrastructure. For this, we need to move on IPv6 addressing mechanism (for large number of sensors and smart devices/things to be connected to the Internet) for each IoT device. Note that IPv6 is a technology/addressing scheme (in network) considered most suitable for IoT, as it offers scalability, flexibility, tested, extended, ubiquitous, open, and end-to-end connectivity. Hence, it is a major challenge for IoT devices to move this addressing (new) scheme (IPv6).
- b. Data and Information: The large volume of data (generated by several IoT devices) presents a biggest challenge for service providers in an IoT ecosystem. Big Data is being so important and useful to organizations [13]. For that, we need to overcome challenges like storing information at a secure place, and by a secure mechanism, which will be a boost to IoT service providers with analyzing this data, and discovering relevant trends and patterns.
- c. Computer Attacks: These attacks are the most common threats in an IoT/Cloud Environment. Some attacks can be like Denial of Service (DoS), DDoS, etc. spread malware in IoT devices. With such attacks, attackers exploit, or attacks on the user's privacy or even modification of the electronic components of the device. Note that Server and computer security come under this challenge.

- d. **Software Vulnerabilities:** This is also a major security challenge in the vulnerabilities of IoT applications and software. These softwares must be updated (at regular interval), analyzed, tested and configured correctly to prevent security problems (i.e., in platform and backend). Note that Operating Systems (OS) security vulnerability comes under this challenge.
- e. **Data Interception:** Cyber security introduces for preventing any interception to communications (between IoT devices). Session kidnappings, or communication protocols and capturing network data are some (few) threats to which it is essential to adopt standard security measures. Note that Data security comes under this challenge.
- f. **Data Privacy:** IoTs taking the responsibility of data collection, storage and analysis mechanisms to a greater scale. There are several devices which are connected to the Internet and also several elements that require protection, i.e., the device itself, the network, the application or the platform that it uses. As discussed above, some manufacturers of smart devices like mobile, TVs, etc., collect data about their customers to analyse their viewing habits (based on particular timing or trends) so this collected data (by smart TVs/smart phone, etc.) may have a challenge for data privacy during transmission.
- g. **Technical Vulnerabilities in Authentication:** IoTs work with devices (having multiple natures) which are connected to the Internet and collect user data in a cloud through their tool itself. Here, we need to work in depth on the authentication mechanisms to ensure the privacy of the user/protecting user's information against any attacks.
- h. **Data Encryption:** The transmission of data (by non-encrypted) having a major security problem which is an important concern in network security. Now days, Data security is a biggest challenge for a computing environment/IoT ecosystem. While transmitting data seamlessly, it is important to hide from observing devices on the internet.
- i. **Complex System:** The more devices, people, interactions and interfaces, the more the risk for data security raised (system has more variety and diversity). Hence, challenge of managing all points in a network to maximize security also increases.
- j. **Technical Concerns:** We require to increase network capacity, i.e., which can carry more data throughout the network because of the increased usage of IoT devices in everyday life/for every work (like automation, parking, manufacturing, etc.). These devices are generating a lot of data, which will also increase (day by day). Hence, there is a higher need to increase network capacity. Hence, it is also a challenge to store this large amount of data (i.e., Big Data) for final storage and further analysing (for determining useful decision).
- k. **Lack of Common Standard:** Many standards are being used for IoT devices, i.e., no unique standard is available (by IoT manufacturing industries). Hence, it is a big, serious and major challenge to find difference between genuine (permitted) and non-certified (non-permitted) devices connected to the World Wide Web/Internet.

Hence from above discussion, we get to know about several issues and challenges in IoTs. In general, IoTs is a relatively new technological advance. Ignorance of IoT security, both by companies and individual users, also increases the risks of cyber-

security due to lack of experience and the human factor. Apart from above points, some other challenges in IoTs are: Insufficient testing and updating, Brute-forcing and the issue of default passwords, IoT malware, Ransomware, WannaCry, IoT botnets aiming at Cryptocurrency, Data security and Privacy issues (mobile, web, cloud). Small IoT attacks can be prevented for providing efficient Detection, Artificial Intelligence and Automation, Ubiquitous data collection, Potential for unexpected uses of consumer data. Generally, these internet connected devices have capability to make human being lives easier, better and longer. So, if these issues/challenges (or issues) not addressed or solved in near future then these (IoT) devices may lead to a lot/more problems than they are useful (giving benefits) to human beings.

Hence, this section discusses several challenges faced with internet of things like preserving privacy and maintaining security, not having good standards for IoT devices, etc. Now in continuing with this, next section will provide some solutions to secure an IoT ecosystem.

4 Securing Internet of Things Ecosystem

In near future, Internet of Things will be a game changer for several applications, including business. But together this, security and privacy issues will also raise on a larger scale and will require attention from manufacture/research communities. In general, IoT security depends on the ability to identify devices, protecting IoT hosting platform, and protecting data (collected by smart/IoT devices) and share this data with Trusted IoT Device (a trusted device is required to be reliably identifiable and associated with a manufacturer/provider. IoT devices should be able to communicate with the intended/authorized hosting services) and Trusted IoT Master. Here a trust master has the knowledge about secure communication with several embedded sensors (in devices/products), and issues regarding to software (i.e., when it needs to be updated and when not). Note that this updation to these devices keeps them securely (with assurances that using code/services are authentic, unmodified and non-malicious). Sharing information with trusted entities only increase trust among users and on technology. Now, here we are discussing all necessary tasks/components to require/secure an IoT ecosystem.

4.1 Maintaining Data Integrity with Internet of Things

Now days several insurance companies are installing IoT devices on vehicles and collecting data about health and driving status in order to take decisions about insurance claim. But, this data may leak to some other unknown/malicious user. Also, as sensitive data in-transit travels through the IoT cloud hosting, it should be encrypted in network layer to prevent interception. Hence, stored data (captured by devices) should be in active-active mode and seamlessly encrypted to avoid data theft (and leaking of data). Blockchain Technology (first time used in Bit coin: A Crypto- currency [14], in 2009) can be used to fulfil this wish, i.e., can provide higher security to a distributed, decentralized and centralized system.

4.2 Establishing Trusted Identity Internet of Things

As discussed above, IoT is built on a network of uniquely identifiable devices, whereas, public key cryptography plays a biggest role in establishing trusted identities (in IoTs). Public key cryptography used a concept of using two different keys to share any information among systems/users. Where one of the key is made public (i.e., public key) and the other is kept private (i.e., private key). Information can be read if both of the keys apply correctly on encrypted information. It is also called asymmetric encryption because it uses one key for encrypting and other one for decrypting. This process is done by a Certification Authority (CA), via issuing a digital certificate to confirm the authenticity of a device. Similarly, a digital certificate contains several fields that help in establishing and validating the identity of a device/system (related to a corresponding public key). These certificates will be used to identify devices, sign firmware /software updates, and facilitate encrypted communications, i.e., to provide sufficient level of security to passes/stored information. Also, trust can be built via creating blocks and storing encrypted information in blocks with consisting information with respect to previous and next block's records (i.e., a Blockchain concept) in an IoT environment.

4.3 Establishing a Public Key Infrastructure for Internet of Things

As discussed above, identity infrastructure is built on both/combination of public and private keys. Note that in asymmetric key cryptography, public keys are freely available for all, but the private keys kept as secret and secure (must be). If a private key is not kept secure/private, then credibility of respective key may get compromised. The secure generation and storage of these keys is paramount. Public Key Infrastructure (PKI) (an Asymmetric Key Cryptography) need to be secured by a novel propped solution (which is properly implemented with some real world attacks) against tamper-resistant hardware /to protected stored data. Using this mechanism, we can easily mitigate an attacker/attack in a network.

4.4 Protecting Aggregated Big Data with Encryption

The data collected, transmitted, and stored in clouds/IoT can be protected using encryption mechanisms. Providing confidentiality to large data can be achieved by good encryption mechanisms (like digital signature, etc.). For that, we can use Blockchain technology to secure this data, i.e., storing this data in blocks (after encrypt) then make a connection with next blocks (according to data/information). A data is situated in two forms (in a cloud/IoTs communication) like data at rest (static) and data in mode (dynamic).

- i. Protection of Data at Rest: When IoTs devices are communicating, then they generating a lot of data, which is stored at several locations with secure mechanisms. Encrypting this data and keeping it at server side provides scalable, cost effective storage, and fast processing in near future. These encryption mechanisms provide availability, integrity and usage of respective collected data (i.e., accessible all time to users). Note that this data is stored at several locations in form of clusters

(across multiple of data nodes) in unprotected manner. So, storing this data with protected manner and avoiding any possible entry point to any malicious users/insider is an essential issue to overlook/focus in near future. To overcome this issue of protecting stored data, firms/organizations need to use sufficient encryption mechanism (after compression of data)/lock down sensitive data at rest in big data clusters (without affecting systems/devices performance). For that, it requires transparent and automated file-system level encryption that is capable of protecting sensitive data at rest on these distributed nodes.

- ii. Protection of Data in Motion: Encrypting communicated data (moving through IoT ecosystem) presents a unique challenge because it has a high variety and increasing at a higher rate. As data (from a device) moves from one location to another (to another device), it is highly vulnerable to attacks like fibre tapping attack, man in middle attack, etc. Note that an attacker can listen a communication (which is being with two parties/devices) with tempering/attaching a cable (with fibre coupling device) and no device (or mechanism) can detect it. This attack is looks like insider-attack (a type of active attack). In this, attacker can record all activity that runs across a network, and data is captured and stolen without the owner's knowledge (even sender and receiver's knowledge). In worst case, this type of attack can also be used to change data, and has potential to override the controls on the entire system. IoTs communication (over public networks) will require to be secured via similar ways we protect other communications over the Internet, i.e., using Transport Layer Security (TLS). Note that encryption is also required at the back-end infrastructure level of manufacturers, cloud service providers, and IoT solution providers.

A data can also be protected using Blockchain concept. Security can be provided to any types of data via creating blocks and storing encrypted data/information in blocks with consisting information with respect to previous and next block's records. This process is clearly impossible to compromise (except in case of covering majority of blocks) by any attacks. Hence this works presents several suggestions or techniques to (provide security) securing an IoT ecosystem in an efficient manner. Now, next section will discuss several possible ways to avoiding a user from being trapped by IoTs devices (with a real world example).

5 What Can We Do?

Today's IoTs are creating environment like cyber physical systems, where researcher are looking for cyber security but they do not look over the physical security of systems/devices. When attacks are happening on any IoT devices, they we need to protect these devise with possible encryption mechanism and efficient symmetric or asymmetric cryptography key to strengthen the security of IoT devices/environments. Also, we can use security tools like data encryption, strong user authentication, resilient coding and standardized and tested APIs (Application Programming Interface). Also, we need to look over security of physical space (including cyber space), i.e., Physical security is also an issue here, since these devices are usually used in open (like in smart

metering, smart transportation, etc.) or in remote locations and anyone can get physical access to it. This kind of issue requires much attention from research community. Note that some security tools need to be applied directly to the connected IoTs devices. In this era, traditional computers, the IoT and its cousin BYOD (Bring Your Own Device) have similar security issues. These IoT devices do not have any sufficient capability to defend themselves (automatically) and need to be protected via some external software like firewalls and intrusion detection/prevention systems. Creating a separate network like virtual private network or any private network is also a solution, but with large number of devices, it fails. Also, protecting devices with firewalls also fails in case of software updating for next version (due to timely security updates on the devices). At updating time, any attacker can sense or enter in a device. Hence, securing IoT is more difficult from other types of security initiatives (like physical security). When someone has physical access to the device once, the security concerns raise automatically. When we evaluate security of IoT or protect data in IoT, then we get that this technology is still in progress very much. In summary, losing of privacy, security or trust is always start with user's permission only. Hence, using/at the time of configuring IoT devices, a user need to be more careful and aware about not to every location/information of himself.

Hence in this section, we discuss the ways, through which, we can protect ourselves in this smart worlds/era (in connection of IoTs), i.e., provide several solutions for avoiding tracking by IoTs or not being trapped with IoTs devices. Now next, sections will conclude this work in brief with few future remarks.

6 Conclusion

Today's Internet of Things is emerging as a big revolution (third wave) in the development of the Internet. Note that in the past, in 1990s' (as first wave), Internet wave connected 1 billion users, while in 2000s', mobile connected another 2 billion users (as another wave). The Internet of Things has the potential to connect 10X as many (28 billion) "things" to the Internet by 2020, ranging from bracelets to cars. This paper reveals that due to the decreasing the cost of sensors, processing power, smart things are getting cheaper and cheaper. Also, several governments (like Japan, Australia, Dubai, India) are pushing to use the applications of IoTs devices like smart home, smart cities, smart transportation, smart grid, etc. Dubai will fully upgraded before 2022 with smart things/devices. In India, concept of smart cities is already launched and Amravati city is going to be the first India's smart city before 2022. Apart that, we also reveal that now days several smart objects/things like smart watches, smart specs, and thermostats (Nest), etc., are already getting attention from public users. But, using such devices/rising of IoTs creates several serious issues about privacy, security, safety, etc. Now, this work worried about user's privacy, i.e., IoT devices/smart gadgets (which is configured badly) might provide a backdoor for hackers/strangers to look/in to break into corporate networks/personal life of respective user. Hence, preserving user's privacy, security at the device level, protecting the master, and encrypting communication links are critical to the secure operations of IoTs. In summary, security needs to be built in as the foundation of IoT systems, with rigorous validity checks,

authentication, data verification, and all the data needs to be encrypted. Also, user's privacy needs to be persevered with new algorithms/mechanism.

References

1. https://en.wikipedia.org/wiki/Tim_Berners-Lee
2. Tyagi AK, Nandula A, Rekha G, Sharma S, Sreenath N (2019) How a user will look at the connection of internet of things devices?: a smarter look of smarter environment. In: ICACSE: 2019: 2nd international conference on advanced computing and software engineering, KNIT Sultanpur, India, 8–9 February 2019
3. TELEFÓNICA I + D: Internet of Things + Internet of Services (2008)
4. <https://wikisites.cityu.edu.hk/sites/netcomp/articles/Pages/InternetofThings.aspx>
5. Tyagi AK, Shamila M (2019) Spy in the crowd: how user's Privacy is getting affected with the integration of internet of thing's devices. In: SUSCOM-2019: International conference on sustainable computing in science, technology & management (SUSCOM-2019). Amity University Rajasthan, India, 26–28 February 2019
6. <https://datafloq.com/read/internet-of-things-iot-security-privacy-safety/948>
7. <https://www.pcworld.com/article/2884612/security/internet-of-things-security-check-how-3-smart-devices-can-be-dumb-about-the-risks.html>
8. <https://www.theguardian.com/technology/2015/aug/12/hack-car-brakes-sms-text>
9. AmirGandomi Murtaza Haider (2015) Beyond the hype: big data concepts, methods, and analytics. *Int J Inf Manag* 35(2):137–144
10. <https://techdifferences.com/difference-between-active-and-passive-attacks.html>
11. Hunt R (2004) Network Security: the Principles of Threats, Attacks and Intrusions, part1 and part 2, APRICOT
12. Veerendra GG, Hacking Internet of Things (IoT), A Case Study on DTH Vulnerabilities, SecPod Technologies
13. <https://datafloq.com/read/big-data-history/239>
14. Nakamoto S, Bitcoin: A peer-to-peer electronic cash system. <http://bitcoin.org/bitcoin.pdf>
15. Tyagi AK, Aghila G (2011) A wide Scale survey on Botnet. *Int J Comput Appl* 34(9), 9–22, November (ISSN: 0975-8887)