A Survey on IoT related Security Issues, Challenges And their Solutions

[1]Ms.Bhagyashri A Bhandari, [2]Ms.Jareena N Shaikh,
[1,2]Lecturer,[1,2]Computer Engg. Dept. , JSPM's Bhivrabai Sawant Polytechinc, Wagholi, Pune, Maharshatra, India. [1]*bhagya.wankar@gmail.com*, [2]*jareenanshaikh@gmail.com*

Abstract- The future of Internet of Things (IoT) is already upon us. The Internet of Things (IoT) is the ability to provide everyday devices with a way of identification and another way for communication with each other. The spectrum of IoT application domains is very large including smart homes, smart cities, wearables, e-health, etc. Consequently, tens and even hundreds of billions of devices will be connected. Such devices will have smart capabilities to collect, analyze and even make decisions without any human interaction. Security is a supreme requirement in such circumstances, and in particular authentication is of high interest given the damage that could happen from a malicious unauthenticated device in an IoT system. While enjoying the convenience and efficiency that IoT brings to us, new threats from IoT also have emerged. There are increasing research works to ease these threats, but many problems remain open. To better understand the essential reasons of new threats and the challenges in current research, this survey first proposes the concept of "IoT features". Then, the security and privacy effects of eight IoT new features were discussed including the threats they cause, existing solutions and challenges yet to be solved.

Keywords - internet of things; security; privacy; confidentiality; challenges.

I. INTRODUCTION

Internet of things (IoT) is a collection of many interconnected objects, services, humans, and devices that can communicate, share data, and information to achieve a common goal in different areas and applications. IoT has many implementation domains like transportation, agriculture, healthcare, energy production and distribution. Devices in IoT follow an Identity Management approach to be identified in a collection of similar and heterogeneous devices. Similarly, a region in IoT can be defined by an IP address but within each region each entity has a unique.

The purpose of IoT is to transform the way we live today by making intelligent devices around us perform daily tasks and chores.There are many application domains of IoT, ranging from personal to enterprise environments [1]. The applications in personal and social domain enable the IoT users to interact with their surrounding environment, and human users to maintain and build social relationships. Another application of IoT is in transportation domain, in which various smart cars, smart roads, and smart traffic signals serve the purpose of safe and convenient transportation facilities. The enterprises and industries domain encompass the applications used in finance, banking, marketing etc. to enable different inter- and interactivities in organizations.

The IoT applications have seen rapid development in recent years due to the technologies of Radio Frequency Identification (RFID) and Wireless Sensor Networks (WSNDue to WSN, each "thing" i.e. people, devices etc. becomes a wireless identifiable object and can communicate among the physical, cyber, and digital world [1].

II. AIMS AND OBJECTIVE

A) Aim

The aim of making this project is to provide an overview of security principles, technological and security challenges, proposed counter measures, and the future directions for securing the IoT and to help the researcher to address the security measures for IOT layers.

b) Objective

- To make IoT services more secure.
- To help the researchers to improve IoT services.
- To design better IoT devices.

III. IOT ARCHITECTURE

In IoT, each layer is defined by its functions and the devices that are used in that layer. There are different opinions regarding the number of layers in IoT. However, according to many researchers [2-4], the IoT mainly operates on three layers termed as Perception, Network,

 DOI : 10.35291/2454-9150.2020.0317

and Application layers. Each layer of IoT has inherent security issues associated with it. Fig. 1 shows the basic three layer architectural framework of IoT with respect to the devices and technologies that encompass each layer.

A. Perception Layer

The perception layer is also known as the "Sensors" layer in IoT. The purpose of this layer is to acquire the data from the environment with the help of sensors and actuators. This layer detects, collects, and processes information and then transmits it to the network layer. This layer also performs the IoT node collaboration in local and short range networks [3].

B. Network Layer

The network layer of IoT serves the function of data routing and transmission to different IoT hubs and devices over the Internet. At this layer, cloud computing platforms, Internet gateways, switching, and routing devices etc. operate by using some of the very recent technologies such as WiFi, LTE, Bluetooth, 3G, Zigbee etc. The network gateways serve as the mediator between different IoT nodes by aggregating, filtering, and transmitting data to and from different sensors [4].

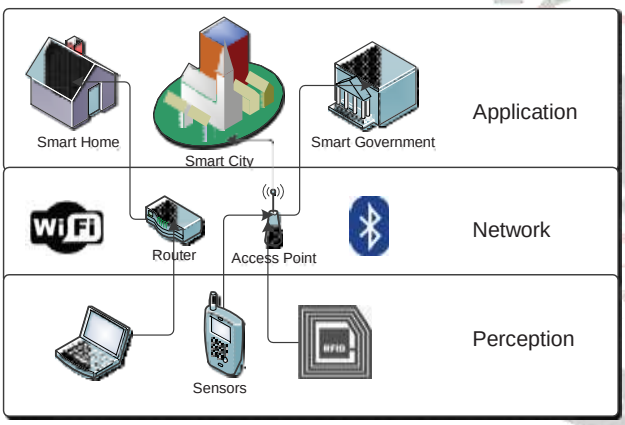

Fig. IOT Architecture

C. Application Layer

The application layer guarantees the authenticity, integrity, and confidentiality of the data. At this layer, the purpose of IoT or the creation of a smart environment is achieved.

IV. IOT SECURITY ISSUES / CHALLENGES

Typical security goals of Confidentiality, Integrity and Availability (CIA) also apply to IoT. The following are the main challenges/isssues of IOT:

A. The Security Challenges of IoT

The security challenges of IoT can be broadly divided into two classes; Technological challenges and Security challenges The technological challenges arise due to the heterogeneous and ubiquitous nature of IoT devices, while the security challenges are related to the principles and functionalities that should be enforced to achieve a secure network. while security challenges require the ability to ensure security by authentication, confidentiality, end-to-end security, integrity etc [4]. There are different mechanisms to ensure security including:

x The software running on all IoT devices should be authorized.

K: When an IoT device is turned on, it should first authenticate itself into the network before collecting or sending data.

L: Since the IoT devices have limited computation and memory capabilities, firewalling is necessary in IoT network to filter packets directed to the devices.

M: The updates and patches on the device should be installed in a way that additional bandwidth is not consumed.

Given below are the security principles that should be enforced to achieve a secure communication framework for the people, software, processes, and things.

1) Confidentiality*:*

It is very important to ensure that the data is secure and only available to authorized users. In IoT a user can be human, machines and services, and internal objects (devices that are part of the network) and external objects (devices that are not part of the network). For example, it is crucial to make sure that sensors don't reveal the collected data to neighboring nodes [6]. One more confidentiality issue that must be addressed is how the data will be managed. It is important for the users of IoT to be aware of the data management mechanisms that will be applied [7].

2) Integrity: The IoT is based on exchanging data between many different devices, which is why it is very important to ensure the accuracy of the data; that it is coming from the right sender as well as to ensure that the data is not tampered during the process of transmission due to intended or unintended interference. The integrity feature can be imposed by maintaining end-to-end security in IoT communication.

3) Availability: The vision of IoT is to connect as many smart devices as possible. The users of the IoT should have all the data available whenever they need it. However data is not the only component that is used in the IoT; devices and services must also be reachable and available when needed in a timely fashion in order to achieve the expectations of IoT.

4) Authentication: Each object in the IoT must be able to clearly identify and authenticate other objects. However, this process can be very challenging because of the nature of the IoT; many entities are involved (devices, people,

 DOI : 10.35291/2454-9150.2020.0317

services, service providers and processing units) and one other thing is that sometimes objects may need to interact with others for the first time (objects they do not know) [8]. Because of all this, a mechanism to mutually authenticate entities in every interaction in the IoT is needed.

5) Lightweight Solutions : Lightweight solutions are a unique security feature that is introduced because of the limitations in the computational and power capabilities of the devices involved in the IoT. It is not a goal in itself rather a restriction that must be considered while designing and implementing protocols either in encryption or authentication of data and devices in IoT. Since these algorithms are meant to be run on IoT devices with limited capabilities, so they ought to be compatible with the device capabilities.

6) Heterogeneity:

The IoT connects different entities with different capabilities, complexity, and different vendors. The devices even have different dates and release versions, use different technical interfaces and bitrates, and are designed for an altogether different functions, therefore protocols must be designed to work in all different devices as well as in different situations [2, 4, 8]. The IoT aims at connecting device to device, human to device, and human to human, thus it provides connection between heterogeneous things and networks [5].

7) Policies:

There must be policies and standards to ensure that data will be managed, protected, and transmitted in an efficient way, but more importantly a mechanism to enforce such polices is needed to ensure that every entity is applying the standards. Service Level Agreements (SLAs) must be clearly identified in every service involved. Current policies that are used in computer and networks security may not be applicable for IoT, due to its heterogeneous and dynamic nature. The enforcement of such policies will introduce trust by human users in the IoT paradigm which will eventually result in its growth and scalability

8) Key Management Systems:

In IoT, the devices and IoT sensors need to exchange some encryption materials to ensure confidentiality of the data. For this purpose, there needs to be a lightweight key management system for all frameworks that can enable trust between different things, and can distribute keys by consuming devices' minimum capabilities.

V. IOT SECURITY COUNTER MEASURES

IoT requires security measures at all three layers; at physical layer for data gathering, at network layer for routing and transmission, and at application layer to maintain confidentiality, authentication, and integrity [4]. In this section the state-of-art security measures that address the specific features and security goals of IoT are discussed.

A. Authentication Measures

In 2011, Zhao et al. in [10] presented a mutual authentication scheme for IoT between platforms and terminal nodes. The scheme is based on hashing and feature extraction. The feature extraction was combined with the hash function to avoid any collision attacks. This scheme actually provides a good solution for authentication in IoT. The feature extraction process has the properties of irreversibility which is needed to ensure security and it is light weight which is desirable in IoT. The scheme focuses on authentication process when the platform is trying to send data to terminal nodes and not the opposite.

Another method for ID authentication at sensor nodes of IoT is presented by Wen et al. in [9]. It is a one-time one cipher method based on request-reply mechanism. This dynamic variable cipher is implemented by using a pre-shared matrix between the communicating parties. The parties can generate a random coordinate which will serve as the key coordinate. Key coordinate is the thing which actually gets transferred between two parties, not the key itself. The key, i.e. password, is then generated from this coordinate. All the messages are sent by encrypting them with the key, along with key coordinate, device ID, and time stamp. The two devices communicate by validating timestamps, and thus they can cancel the session based on it. This cipher can be used where securing IoT is not very sensitive and crucial because key can be repeated for different coordinates. If key coordinate is changed regularly, security can be optimized for that particular IoT framework. The installation of pre-shared matrix needs to be secure for this work to be implemented for a large number of IoT devices.

B. Trust Establishment

Since, devices in IoT can physically move from one owner to another, trust should be established between both owners to enable a smooth transition of the IoT device with respect to access control and permissions. The work in [13] presents the concept of mutual trust for inter-system security in IoT by creating an item-level access-control framework. It establishes trust from the creation to operation and transmission phase of IoT. This trust is established by two mechanisms; the creation key and the token. Any new device which is created is assigned a creation key by an entitlement system. This key is to be applied for by the manufacturer of the device. The token are created by the manufacturer, or current owner, and this token is combined with the RFID identification of the device. This mechanism ensures the change of permissions by the device itself if it is assigned a new owner, or it is

 DOI : 10.35291/2454-9150.2020.0317

going to be operated in a different department of the same company, thus reducing the overhead of the new owner.

C. Federated Architecture

Not having universal policies and standards to control the design and the implementation of algorithms in IoT makes it difficult to control the security. It is important for IoT architecture to have a federated architecture that has an internal autonomy or centralized unit to overcome the heterogeneity of various devices, software's and protocols. Such attempt was made in [15] to propose a framework called Secure Mediation GateWay (SMGW) for critical infrastructures. This approach is an abstraction of IoT as it is relevant for any kind of distributed infrastructures that are completely different in their nature and operation. SMGW can discover all the relevant distributed information from different nodes, and can overcome the heterogeneity of heterogeneous nodes whether it is a telecommunication, electrical, water distribution node, and can exchange all the messages and information over the untrusted network of Internet.

It is not enough to have policies and standards to ensure security, mechanisms to enforce such policies are also needed. The research by Neisse et al. in [16] addresses this issue by integrating a security toolkit named SecKit with the MQ Telemetry Transport protocol. The current policies may not be efficient in IoT because of its dynamic nature. The proposed policy mechanism can have good impact in ensuring the security of the IoT, however it introduced additional delay in the process.

D. Security Awareness

Another important security measure for the success and growth of IoT framework is the awareness among human users which are a part of the IoT network. In [17] the authors explained the consequences of not securing the IoT using actual numbers. They accessed IoT devices (SCADA devices, web cameras, traffic control devices, and printers) that were publicly available using either no-password or the default password. The recorded results were very interesting and showed that many of these devices were actually accessible.

VI. CURRENT STATUS OF RESEARCH

IoT security is determined by the many factors and security principles discussed earlier, and the challenges that are faced by IoT security has been the focus of many researchers. In this section, an analysis of some related work is presented and the contribution of this paper is given.

In the survey paper presented by Roman et al. in [7], a detailed introduction about the IoT and security issues along with the need to have IoT standards are addressed. However, no countermeasures are provided for the given security challenges. This work was followed by the survey analysis in which counter measures are provided for all security challenges. However, global policies for securing IoT and computational resources of security solutions w.r.t. devices are not provided. The analysis in [1] addresses the security threats, challenges, and requirements in detail, but presents state-of-art countermeasures for only one security feature of access control. In [6], IoT security in terms of the main principles of security like confidentiality, integrity, and availability are addressed only. The authors suggested two-step authorization using biometrics which is not applicable in case of machine-to-machine communication. The suggested measures are not detailed and do not address the specific nature of IoT with low power heterogeneous devices and huge network traffic. A very good survey for IoT, Web of Things (WoT), Social Web of Things (SWoT) is presented in [18], in which security issues, measures and potential research directions are given. In this survey paper, the security challenges, requirements, and state-of-art measures and research are presented with emphasis on using the latest network protocols like IPv6 and 5G to further secure the IoT paradigm.

Wireless Internet Service Provider (WISPr) roaming and RADIUS are existing solutions to provide authentication and authorization in IoT by means of Wi-Fi over the Internet. Today, many smart devices support IPv6 communications, but the existing deployments in IoT might not support it , and thus requires ad hoc gateways and middlewares [11]. The survey shows that open research challenges are present to achieve centralized autonomy in IoT devices by having a Management Hub which manages the identification management issues in IoT.

VII. ADVANTAGES

- **Security:** You can monitor your home using your mobile phones, with the ability to control it. It can provide personal safety.
- **Stay connected:** You and your family members can always be in the network. You can virtually stay connected.
- **Efficient use of electricity and energy:** If your home appliances are communicating with you about the work done, their maintenance and repair will be easy. If appliances can operate by themselves then electricity utilization will be possible by an efficient way.
- **Health Care and Management** : The patient monitoring is possible on a real time basis without doctor's visit and also enables them to make decisions as well as offer treatment when emergency is there.
- **Cost-** Effective Business Operations: A large number of business operations like shipping and location,

 DOI : 10.35291/2454-9150.2020.0317

security, asset tracking and inventory control, individual order tracking, customer management, personalized marketing & sales operations etc. can be done efficiently with a proper tracking system using IoT .

VIII. DISADVANTAGES OF IOT

- **Privacy issues:** Hackers can break into the system and possibility of stealing the data.
- **Becoming Indolent:** People are more habituated to have a click based work making them lazy to any sort of physical activity, applied science in their daily routine.
- **Unemployment:** Lower level people like unskilled labour may have high risks of losing their jobs.

IX. COMPARATIVE STUDY

Table : Comparative Study

Year	Author	Problem	Solution
2016	K. Zhao and L. Ge [2]	Multimedia traffic security	• Media-mindful Traffic Security Architecture (MTSA) was proposed • MTSA is empowered with apparent mixed media mutilation methods. • The MTSA lessens the multifaceted nature of sight and sound calculations and diminishes the size of the offers MTSA is acquired from a setting mindful media administration based security structure
2011	Roman et al [7]	End-to-End security	• Using the Datagram Transport Layer Security (DTLS) convention, in light of the most generally utilized open key cryptography strategy (RSA),
2014	M. Leo, F. Battisti [4]	Cyber-physical-social security	• by the Unit IoT and Ubiquitous IoT (U2IoT) design. • U2IoT give three key backings, for example, setting up data security model to portray the mapping relations among U2IoT, security layer, and security necessity in which social layer and extra knowledge and similarity properties are mixed into
2015	M. Farooq, M. Waseem, [5]	Hierarchical security	• The proposed progressive security engineering to ensure against natural receptiveness, heterogeneity, and terminal weakness. • The proposed engineering expects to improve the proficiency, unwavering quality, and controllability of the whole security framework.
2012	Q. Wen, X. Dong,.[9]	• Object security • Should be content- centric	• Object-based Security Architecture (OSCAR). • Authors assess OSCAR in two cases: (a) 802.15.4 Low Power empowered Lossy Networks (LLN), and (b) M2M correspondence for two diverse equipment stages and MAC layers

X. FUTURE SCOPE

IoT has seen rapid development in recent years in the areas of Telemedicine platforms, Intelligent Transportation systems, Logistics Monitoring, and Pollution Monitoring Systems etc.The security challenges related to the IoT must be dealt with to achieve its growth and maturation. Given below are future directions for research in order to make the IoT paradigm more secure.

A. Architecture Standards

IoT currently employs different devices, services, and protocols to achieve a common goal. However, to integrate a network of IoT frameworks to achieve a bigger framework, for example, to form a smart town by the integration of many smart homes, there needs to be a set of standards that should be followed from the micro to macro levels of IoT realization. The present day requirement of IoT is to have well defined architecture standards comprising of data models, interfaces, and protocols which can support a wide range of humans, devices, languages, and operating systems.

B. Identity Management

Identity management in IoT is performed by exchanging identifying information between the things for first time connection. This process is susceptible to eavesdropping which can lead to man-in-the-middle attack, and thus can jeopardize the whole IoT framework. Hence, there needs to be some pre-defined identity management entity or hub which can monitor the connection process of devices by applying cryptography and other techniques to prevent identity theft.

C. Session layer

As per most of the researchers, the three-layer architecture of IoT does not accommodate the opening, closing, and managing a session between two things. So, there is a need for protocols which can address these issues and can ease the communication between devices. An abstract session

 DOI : 10.35291/2454-9150.2020.0317

layer should be accommodated as an additional layer in IoT architecture which can specifically manage the connections, protocols, and sessions between communicating heterogeneous devices.

D. 5G Protocol

To realize the implementation of IoT, IPv4 will definitely fall short in accommodating the huge numbers of IP-identifiable objects. That is the reason why people are now heading to IPv6, which is able to support $3.4x10^{38}$ devices. However, such number will create huge amount of traffic, which can lead to more delay and thus more bandwidth is needed. The expectation of the new generation of communication (5G) is to provide speed between 10-800Gbps, comparing this number with the current technology (4G) with speed of 2-1000 Mbps, 5G should be able to handle the traffic produced by IoT devices. The implementation of 5G will be defined by many current and developing technologies such as: Heterogeneous Networks (HetNets), Software Defined Networks (SDNs), Massive MIMO, and Multiple Radio Access etc [20]. However, all these technologies come with their own security challenges. For example, HetNets will have frequent handover which directly affects the authentication process in the network, especially with the small latency requirement of 5G. Also, cloud computing and SDNs will increase the numbers of DDoS attacks due to the On-Demand Self-Service characteristic of cloud computing. Although [21] addressed the authentication and security of SDN by having a decentralized control of authentication using user-dependent security context, the security of 5G and all the emerging technologies involved in 5G must be extensively addressed, in order to ensure IoT security.

XI. CONCLUSION

This paper presents taxonomy and a literature review of challenges and security in the context of IoT.

The analysis of a large spread of security challenges to identify a number of requirements that should be taken into consideration by researchers and developers while developing new security schemes for IoT networks and their applications.

The IoT framework is susceptible to attacks at each layer; hence there are many security challenges and requirements that need to be addressed. Current state of research in IoT is mainly focused on authentication and access control protocols, but with the rapid advancement of technology it is essential to incorporate new networking protocols like IPv6 and 5G to achieve the dynamic mashup of IoT topology.

The major developments witnessed in IoT are mainly on small scale i.e. within companies, some industries etc. To scale the IoT framework from one company to a group of different companies and systems, various security concerns need to be overcome. The IoT has great potential to transform the way we live today. But, the foremost concern in realization of completely smart frameworks is security. If security concerns like privacy, confidentiality, authentication, access control, end-to-end security, trust management, global policies and standards are addressed completely, we can witness the transformation of everything by IoT in the near future. There is need for new identification, wireless, software, and hardware technologies to resolve the currently open research challenges in IoT like the standards for heterogeneous devices, implementation of key management and identity establishment systems, and trust management hubs.

REFERENCES

[1] M. Abomhara and G. M. Koien, "Security and privacy in the Internet of Things: Current status and open issues," in *Int'l Conference on Privacy and Security in Mobile Systems (PRISMS)*, 1-8, 2018.

[2] K. Zhao and L. Ge, "A survey on the internet of things security," in *Int'l Conf. on Computational Intelligence and Security (CIS)*, 663-667, 2016.

[3] L. Atzori, A. Iera, G. Morabito, and M. Nitti, "The social internet of things (siot)–when social networks meet the internet of things: Concept, architecture and network characterization," *Computer Networks*, vol. 56, 3594-3608, 2017.

[4] M. Leo, F. Battisti, M. Carli, and A. Neri, "A federated architecture approach for Internet of Things security," in *Euro Med Telco Conference (EMTC)*, 1-5, 2014.

[5] P. N. Mahalle, B. Anggorojati, N. R. Prasad, and R. Prasad, "Identity authentication and capability based access control (iacac) for the internet of things," *J. of Cyber Security and Mobility*, vol. 1, 309-348, 2013.

[6] M. Farooq, M. Waseem, A. Khairi "A Critical Analysis on the Security Concerns of Internet of Things (IoT)," *Perception*, vol. 111, 2015.

[7] R. Roman, P. Najera, and J. Lopez, "Securing the internet of things," *Computer*, vol. 44, 51-58, 2011.

[8] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," *Computer Networks*, vol. 57, 2266-2279, 2013.

[9] Q. Wen, X. Dong, and R. Zhang, "Application of dynamic variable cipher security certificate in internet of things," in *Int'l Conference on Cloud Computing and Intelligent Systems (CCIS)*, 1062-1066, 2012.

[10] G. Zhao, X. Si, and T. Hu, "A novel mutual authentication scheme for Internet of Things," in *Int'l Conference on Modelling, Identification and Control (ICMIC)*, 563-566, 2011.

[11] J.-Y. Lee, W.-C. Lin, and Y.-H. Huang, "A lightweight authentication protocol for internet of things," in *Int'l Symposium on Next-Generation Electronics (ISNE)*, 1-2, 2014.

 DOI : 10.35291/2454-9150.2020.0317