A Survey on Security Issues in IoT

D. J. Joel Devadass Daniel
AP, Department of Electronics and Communication Engineering, JACSICE, Nazareth, Tuticorin District, Tamil Nadu, India.

Dr. S.Ebenezer Juliet
ASP, Department of Computer Science and Engineering, VV College of Engineering, Tisaiyanviali, Tuticorin District, Tamil Nadu, India

Abstract – Internet of Things is a combination of digital and physical entities that can be linked, using information and communication technologies, to enable various applications and services.It's an developing worldwide Internet-based technical architecture that provides exchange of goods and services in global supply chain networks has an impact on the security and privacy of the involved stakeholders. In IoT, the gratification of security and privacy needs plays a vital role. Such demand include data confidentiality and access control, authentication within the IoT network, privacy and trust within the users and things, and the enforcement of security and privacy policies. In this article, we present a survey on various issues in security for Internet of Things.

Index Terms – IoT, Security and Privacy, Access Control, Authentication.

1. INTRODUCTION

Over the last couple of decades, the Internet has been in a firm state of evolution. While there is no universal definition for the IoT, the core concept is that everyday objects can be equipped with identifying, sensing, networking and processing capabilitiesthat will allow them to communicate with one another and with other devices and services over the Internet toachieve some useful objective. The machine-to-machine communication is also not new idea, it is basic idea of the Internet where clients, servers and routers communicate to one another. IoT in general represents the evolution of the utilization of existing technologies and kinds of devices and interconnection of networks.1 The Internet of Things is a idea in which the virtual world of information and communication technology merges with the real world of things. The real world becomes more accessible Through computers and networked in everyday scenarios. management can start to move freely from macro to micro levels with access to fine-graind information's and will be able to measure, plan and act accordingly.

The Internet of Things is more efficient and more effective– it also enable a more easy way of life.2 The Internet of Things (IoT) is a developing global Internet based information architecture facilitating the exchange of goods and services in global supply chain networks. The IoT has the purpose of providing an IT-infrastructure facilitating the exchanges of ''things'' in a secure and reliable manner. 3

'A worldwide network of interconnected entities'. In most cases, these heterogeneous entities, 'things' (e.g. Human beings and computers, books and cars, appliances and food) have a locatable, addressable, and readable counterpart on the Internet. Many technologies serve as the building blocks of this new paradigm, such as wireless sensor networks (WSNs), RFID, cloud services, machine-to-machine interfaces (M2M), and so on. Also, this paradigm has a multitude of application domains, such as automotive, healthcare, logistics, environmental monitoring, and many others. ''The Internet of Things concept will take more than a decade to reach the peak of Productivity – mainly due to the security issues. security risks are annoyed by the trend toward a separation of sensor network infrastructure and applications .so its must that , a true end-to-end security solution is needed to attain an sufficient level of security for the IoT. Protecting the data once it leaves the scope of the local network is not enough.5

From a logical viewpoint, an IoT system is one by which a common goal is attained by the collection of smart devices that interact on a collective basis. it is mandatory to define valid security, privacy and trust models suitable for the IoT. With reference to security, data anonymity, confidentiality and integrity need to be guaranteed, as well as authentication and authorization mechanisms in order to prevent unauthorized users (i.e., humans and devices) to access the system Many aspects of our lives are already impacted by this technology yet it is challenging industry, communications, health, economics, business models, IT, and securityMany aspects of our lives are already impacted by this technology yet it is challenging industry, communications, health, economics, business models, IT, and security7.

2. IOT GENERAL ARCHITECTURE

Generally, the structure of Internet of Things (IoT) I divided into four layers as shown in Fig.1. The general layered architecture of the IoT and its constituent elements have been discussed:

A. *Perception Layer*

This layer is also known as the sensing layer. The application of intelligent sensors simplifies the connectivity among objects, besides facilitating the exchange of information amongst them. This layer consists of integrated hardware for perception and acquisition of data. Most popular sensing technologies have been discussed [1]:

1) RFID

In the paradigm of embedded communications, RFID has been a major breakthrough, thus enabling design of microchips for wireless communications. They can be embedded into objects for enabling their automatic identification. RFID tags may be passive or active. The passive RFID tags have no internal power whereas the active RFID tags are self-powered and can initiate the communication as well. The passive RFID tags are being increasingly deployed in transportation, retail, logistics, road toll tags and bank smartcards, whereas the active RFID tags find applications in auto manufacturing and remote monitoring.

2) WSN (Wireless Sensor Networks)

With the recent advancements in nano technology, wireless communications and low power integrated circuits, miniature devices are now available at much lower costs, providing much higher efficiency and also ensuring low energy consumption in remote sensing applications.

This has allowed for the implementation of wireless sensor network by deploying multitude of intelligent sensor nodes, thus enabling the acquisition, processing, analysis and dissemination of useful information, collected across the network [4]. The sensed information is shared among the sensors and then sent for processing, storage and analytics.

B. *Middleware Layer*

This layer is interposed between the network and application layer, aiming to hide the hardware details and it allows the developers to focus on the application development process. It is responsible for providing services to the customers, besides ensuring interoperability, scalability and abstraction. Also, it authenticates the users to provide a more secure environment along with efficient delivery of services.10

1) Data Storage and Analytics

IoT results in generation of huge volumes of data. Thus, the issues of data storage and analytics gain significance. Presently, the internet is consuming about 5% of the total energy being produced worldwide and as the IoT is envisioned to introduce billions of devices across the world, the energy consumption is sure to go up even further. Hence, it becomes pertinent to analyze the efficiency of data centers to ensure intelligent storage and usage of data for smart monitoring and actuation. A centralized infrastructure is preferred to support data storage and analytics in the IoT. Recently, cloud storage is being increasingly leveraged and in the near future,cloud based analytics and visualization solutions are sure to give promising results [10].

2) Visualization

Visualization is another significant aspect for an IoT application which encompasses providing more information to users through a more interactive interface, thus allowing the users to interact with the surrounding environment. Recent advancements in touch screen technology have promoted the production and usage of smart tablets and phones. If the benefits of the IoT revolution are to reach the common man, focus on development of visualization that is attractive, easy to use and understand is required [10].

C. *Network Layer*

The network layer provides the basic support services for secure data transfer over the sensor networks. It is also responsible for aggregating the information from various sources and routing it to correct destinations. It transfers the information over the wireless network technology such as 3G, Wifi, Bluetooth, infrared, etc [10].

1) Data Aggregation

A secure data aggregation method is required for ensuring that reliable data is being collected from sensor nodes across the network [5]. As node failures are frequent in WSNs, the network topology should be capable of healing itself. Ensuring security in the domain of data aggregation is very essential as the network is automatically connected to sensors and protection of networks from unauthorized or malicious users demands attention.

2) Addressing Schemes

In IoT, billions of objects are envisioned to be connected to each other, so it becomes necessary to provide unique identification for each of those objects. An addressing scheme that uniquely identifies objects deployed across the network is a pre-requisite to the success of IoT. The major aspects attached to a unique address include reliability, scalability and uniqueness. Presently, the IPv4 is able to uniquely identify a group of sensor devices distributed geographically, but the individual sensor devices can not be identified uniquely. Also, IPv4 faces several issues such as internet mobility issue which can be easily resolved by implementing the paradigm of IPv6.

The IPv6 is capable of providing unique addresses to billions of devices. IPv6 also provides for remote access of devices along with their unique identification. A notable progress has been the formulation of a light-weight IPv6 addressing scheme that will facilitate the unique identification of household goods.

D. *Application Layer*

This is the topmost layer of the IoT architecture that provides the delivery of all the services in various fields of industry such as automobile, healthcare, education, logistics, agriculture, insurance, media, environmental monitoring etc

APPLICATION LAYER	Smart home	E health
	Green Agriculture	Environmental Moitoring
MIDDLEWARE LAYER	Service Management	Data Provisioning
	Informtion Processing	Ubiquitous Computing
NETWOTK LAYER	GPRS/EDGE	Wireless Technology
	Bluetooth	Secure Transmission
PRECEPTION LAYER	Barcode	RFID

Fig 2.1. IoT General Architecture

3. THE IOT CHALLENGES AND ADDRESSING THEM

The challenges are multiple and interconnected. They relate to the regulatory environment , manufacture, connectivity, interoperability, integration, device vulnerability, as well as privacy and security.

1) Regulatory device environment

The current regulatory environment surrounding traditional devices means that adopting new models of persistent data generation may be a difficult journey given the current timelines from production to implementation and use. The range of devices together with the necessity for trusted and reliable connection are critical to this technology uptake.

2) Technical Debt

There are inherent problems, summarized as "the technical debt" from engineering design, due to the lack of consideration of cyber security threats.

3) Dynamic connectivity

IoT is not a new computing platform, but a new way of using the existing architecture, bringing new security problems and challenges. The issue of dynamic versus static connectivity, with no fixed end points means that many of the usual communication mechanisms for transferring messagessecurely will not work. It is the global nature of the connectivity between devices that is the major security concern. The networks and connections over which data is travelling are often disparate and inconsistent and under the control of many different stakeholders. This means that there are significant challenges in the privacy and governance of this data, as well as its protection and security. At present these connections are highly reliant on trust

4) Device diversity and interoperability

The truly interoperable IoT system where data is both transferred one-to-one and one-to-many connections incorporating exchange of data across multiple interfaces, will require systems to "play nice" with one another . This is essential when you consider that in any data exchange between multiple systems, the combination of interfaces is 2(n-1). Whilst an issue for IoT in general, the ability for each device and exchange point to understand multiple transmission and security protocols is particularly relevant in healthcare. This is compounded further by the need to understand what code systems and terminologies are used with each device. There is no central registry of device capability. This informational representation even using standards, has proven to be difficult in the real world environment with existing data exchange capability . Device management will require directories of devices functionality, protocols, terminologies and standards compliance. The level of "plug and play" interoperability nowcommonplace in non-health areas, is a long way off in the medical device arena.

5) Consistency and data integration

The integration of device-collected data into electronic systems has significant development ahead of it to ensure the integrity of data. In addition, data provenance - where the origin of data received from external systems needs to be established - is required to ensure data quality and authenticity of the information.

6) Privacy

Since many devices collect personal identifiable information, the privacy concerns are compounded when this data is being shared between mobile applications and cloud services connected to the device. The consistent lack of encryption, network misconfiguration, lack of knowledge on what security to implement, and the inability for the device to handle encryption, are some of the reasons for significant privacy concerns.

7) Security

Most security challenges rely on three elements.

Firstly, data availability and ensuring consistent connectivity and access to services. Disruption to network functionality and denial of service attacks can have a major impact on healthcare delivery. Unlike the business sector, the impact is not restricted to reputation, financial loss and customer dissatisfaction,

Further, a common defence-in-depth security measure is redundancy (duplication of devices/equipment, ready to be swapped into a network), Secondly, authentication and identity management to ensure encryption of data in transit, and sufficient authorisation and authentication measures. Many cloud and mobile technologies fail to require sufficiently complex passwords, and this is a serious cause for concern . Thirdly, system integrity through security protection mechanisms such as verification, monitoring and auditing, is vital. In a similar manner to the use of "bring your own device" (BYOD), IoT and its many derivatives were developing before a commonly accepted security framework and standards to address security were available. Indeed, there is little consensus on how to implement IoT security at the device, network or system levels .

8) Device vulnerability

The overall management of IoT is another aspect to be addressed by organizations. It is already difficult to update the hundreds of devices in situ in an environments This is more complex with the software versioning and legacy operating systems used in the majority of devices . The problem will grow as more devices are connected. A further complication will be vulnerabilities from default access credentialing on many devices, and the increasingly common web-based interface access . The problems often occur where we have changed from static connectivity to dynamic connectivity. For instance, healthcare direct messaging is achieved through secure message delivery (SMD) . However, to be efficiently and effectively deployed these current methods use an Endpoint Location Services (ELS), which enables discovery of the messaging endpoints and endpoint capabilities. Similarly, traditional endpoint security where the transmission channels and the endpoints are known, and discoverable, is disrupted with the dynamic nature of IoT. Another issue is the difficulty of detecting computer-based infections affecting on devices. With minimal or no user interface, this detection together with what methods can be employed to debug security incidents, can be problematic . A further problem may be the use of different telecommunications providers who are legally bound to provide information to law enforcement upon request.

4. SECURITY FRAMEWORK

A. Device or node end point physical security

As the IoT nodes are very easily accessible and can be easily tampered or cloned. so it is necessary to provide tamper resistant hardware for these nodes. There should be enough resiliency even if a node is tampered or compromised, and so the other nodes are protected. once the tampered note is detected, the communication with the node will be blocked which leads to the loss of information. The node may be needed to flush all data remotely in extreme case and so illegal malicious nodes access the critical data. By allowing no access to its memory or crypto information from external sources cloning can be prevented.

B. Bootstrapping and setup security

The cipher and other critical information in the nodes should be kept secret while in the process of latching on to a network in the bootstrapping phase. Typical cryptographic information including pre-shared keys and other private keys must not be compromised or stolen., The device may participate in establishing shared keys after the bootstrapping phase is done safely.

C. Authentication, Access control and Accounting

,It is necessary to properly authenticate itself using certificates as well as the destination node to prevent open access to node data before any node communicates with a server. Also justified authorization and access control rules are to be implemented on these nodes to limit them from super user access. Detailed accounting information of the transaction should be logged at the end. By this spoofing, repudiation and privilege elevation attacks can be prevented.

D. Data transmission and storage security

The light-weight crypto algorithms tailored for these resource constrained networks can be used while being transmitted over the network should be made secure. Symmetric key encryptions are faster but PKI infrastructure though being slow allows dynamic key generation and distribution. check codes may be used for integrity checks and to prevent against MITM attacks light-weight hashes and integrity. The nodes can't store huge amounts of data or are capable of doing huge computations and thus off-load them to powerful cloud servers. as they have very less memory.

E. Proxy security

When the datas are transformed from one form to another the proxies will be the major target. By implementing something like a secure DTLS the bridging infrastructure is expected to provide decent transport level

. 4.1. Analysis of distributed IoT features :

Openness. Beyond presenting raw data and other specialized services, an IoT platform can also be flexible enough to allow 3rd parties to develop complex applications through the provision of an API.

•Viability. This property encompasses two concepts: business model (whether it is viable to market this technology) and vendor lock-in (whether a company can take the long-term risk of depending on a particular provider).

•*Reliability*. Not only the IoT architecture must be resilient enough to assure a certain level of availability, but also needs

to provide a performance that is tailored to the specific needs of the applications.

•*Scalability*. Within this paradigm, it is expected that the number of devices and the amount of data generated and processed by those devices will grow exponentially(i.e. the concept of ‘‘data deluge’’). Thus, we have to take scalability and extensibility into account.

•*Interoperability*. Even if the Internet of Things is inherently heterogeneous, all its components must be able to interact with each other. Therefore, it is necessary to achieve service and semantic interoperability, amongst other things.

•*Data Management*. As the different elements of the Internet of Things produce data, either by sensing or by processing, we must take certain design decisions: where the data should be stored? how the data is accessed?

•*Security Issues*. There are various security issues that must be considered in order to achieve a trusted and fault-tolerant IoT: how to protect the communications? how to manage authentication and access control in a world of billions of things? what about the privacy of the users, and the security of the data generated by the things?

5. SECURITY CHALLENGES, CONSTRAINS OF IoT

S.No	SECURITY CHALLENGES	SECURITY CONSTRAINS
1	Identity and authentication	Tamper resistant packaging
2	Access control	Memory constraint
3	Protocol and network security	Computational and energy constraint
4	Privacy	Embedded software constraint
5	Trust and Governance	Dynamic security patch
6	Fault Talerance	

Fig 5.1. Security challenges and Constrains

6. CONCLUSION

The paper provides an explicit analysis of the features and security challenges of the Internet of Things, There are numerous challenges need to be solved.

Customized security and privacy levels to be guaranteed for the real spreading of IoT services . This survey may provide a broad overview about many open issues, and shed some light on research directions in the IoT security field. More in details, a unified vision regarding the insurance of security and privacy requirements in such an heterogeneous environment, involving different technologies and communication standards is still missing. It is necessary to designed and deploye Suitable solutions , which are independent from the exploited platform and able to guarantee: confidentiality, access control, and privacy for users and things, trustworthiness among devices and users, compliance with defined security and privacy policies. Research efforts are also required to face the integration of IoT and communication technologies in a secure middleware, able to cope with the defined protection constraints.

The challenge is creating end-to-end security solutions that can incorporate the security of individual devices as well as the network and information system as a whole. This is currently a major challenge for the IoT.

IoT is a dynamic technology for the coming generation which can be used in all possible areas. All the current technologies, devices, network applications and services will connect with each other on the common IoT platform. In this paper, we have made the current state of the art towards designing an IoT framework highlighting the major security issues and solutions. One of the basic aims in designing the IoT protocols has been to make objects interoperable across all framework but at the same time take care of the security and privacy issues involved in designing such a framework. Achieving these goals will result in the pervasive deployment of IoT in the near future.

REFERENCES

[1] Andrew Whitmore, Anurag Agarwal & Li Da Xu, “The Internet of Things—A survey of topics and trends,” Volume 17, Issue 2, April 2015, pp. 261–274

[2] Dieter Uckelmann, Mark Harrison, Florian Michahelles, “An Architectural Approach Towards the Future Internet of Things,” Architecting the Internet of Things, pp. 1-24

[3] Rolf H. Weber, “Internet of Things – New security and privacy challenges,” Volume 26, Issue 1, January 2010, PP. 23-30

[4] Rodrigo Roman , Jianying Zhou , Javier Lopez b, “On the features and challenges of security and privacy in distributed internet of things,” Volume 57, Issue 10, 5 July 2013, PP. 2266-2279

[5] Thomas Kothmayr , Corinna Schmitt , Wen Hub, Michael Brünig , Georg Carle , “ DTLS based security and two-way authentication for the Internet of Things,” Volume 11, Issue 8, November 2013, PP. 2710-2723

[6] S. Sicari a, A. Rizzardi a, L.A. Grieco b, A. Coen-Porisini a, “Security, privacy and trust in Internet of Things: The road ahead,” Volume 76, 15 January 2015, PP. 146-164

[7] Mohamed Abomhara, Geir M. Køien, “Security and Privacy in the Internet of Things: Current Status and Open Issues,” Privacy and Security in Mobile Systems (PRISMS), 2014 International Conference, May 2014

[8] Subho Shankar Basu, Somanath Tripathy, Atanu Roy Chowdhury, “Design challenges and security issues in the Internet of Things,” Region 10 IEEE symposium, May 2015

[9] Md. Mahmud Hossain, Maziar Fotouhi, Ragib Hasan, "Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things," IEEE World Congress on Services,July 2015
[10] Gurpreet Singh Matharu, Priyanka Upadhyay, Lalita Chaudhary, "The Internet of Things: Challenges & Security Issues," International Conference on Emerging Technologies (ICET), Dec 2014
[11] R. Kotamsetty and M. Govindarasu, "Adaptive latency-aware query processing on encrypted data for the internet of things," in 2016 25th International Conference on Computer Communication and Networks (ICCCN), Aug 2016, pp. 1–7.
[12] S. A. Salami, J. Baek, K. Salah, and E. Damiani, "Lightweight encryption for smart home," in 2016 11th International Conference on Availability, Reliability and Security (ARES), Aug 2016, pp. 382–388.
[13] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of things: Security vulnerabilities and challenges," in 2015 IEEE Symposium on Computers and Communication (ISCC), July 2015, pp. 180–187.
[14] E. Ronen and A. Shamir, "Extended functionality attacks on iot devices: The case of smart lights," in 2016 IEEE European Symposium on Security and Privacy (EuroS&P), March 2016, pp. 3–12.
[15] O. Salman, S. Abdallah, I. H. Elhajj, A. Chehab, and A. Kayssi, "Identity-based authentication scheme for the internet of things," in 2016 IEEE Symposium on Computers and Communication (ISCC), June 2016, pp. 1109–1111.
[16] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, "Pauthkey: A pervasive authentication protocol and key establishment scheme for wireless sensor networks in distributed iot applications," in International Journal of Distributed Sensor Networks, 2014.
[17] G. Ho, D. Leung, P. Mishra, A. Hosseini, D. Song, and D. Wagner, "Smart locks: Lessons for securing commodity internet of things devices," in Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security, ser. ASIA CCS '16. New York, NY, USA: ACM, 2016, pp. 461–472.
[18] Y. Sharaf-Dabbagh and W. Saad, "On the authentication of devices in the internet of things," in 2016 IEEE 17th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM), June 2016, pp. 1–3.
[19] C. Zhang and R. Green, "Communication security in internet of thing: Preventive measure and avoid ddos attack over iot network," in Proceedings of the 18th Symposium on Communications & Networking, ser. CNS '15. San Diego, CA, USA: Society for Computer Simulation International, 2015, pp. 8–15.
[20] I. B. Pasquier, A. A. Ouahman, A. A. E. Kalam, and M. O. de Montfort, "Smartorbac security and privacy in the internet of things," in 2015 IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA), Nov 2015, pp. 1–8.