A Systematic Study of Security Issues in Internet-of-Things (IoT)

Santhosh Krishna B V [#1]
[#1]Research Scholar
Velammal Institute of Technology
Chennai, Tamil Nadu, India
[#1] santhoshkrishna1987@gmail.com

Gnanasekaran T [#2]
[#2] Professor
RMK Engineering College
Chennai, Tamil Nadu, India
[#2]t.gnanasekaran@gmail.com

Abstract : **Internet of things (IoT), also referred to as the internet of objects, is a dynamic global information network consisting of internet – connected objects. Wireless sensor networks (WSN) and RFID enabled Internet of Things finds a plethora of applications in almost all the fields such as education, health, agriculture, transportation and entertainment. Compact smart devices constitute an essential part of IoT. These compact smart devices range widely in size, energy, use, capacity and computation power. On the other hand, the integration of these smart things into the standard internet introduces several security challenges because the majority of internet technologies and protocols were not designed to support IoT. Though number of researchers have explored about such security challenges and open problems in IoT, there is a lack of a systematic study of the security challenges in the IoT landscape . This paper briefs the motivation for IoT, secured IoT layered architecture, IoT applications, Security issues with various attacks in each layer of the IoT and existing methods for providing security solutions and their limitations.**

Keywords -- RFID ; WSN (Wireless Sensor Networks) ; IoT (Internet of Things) ; Security challenges ; Smart devices; Attacks; Layered Architecture

I. INTRODUCTION

The internet of things (IoT) paradigm has gained popularity in recent years. IoT does not have a unique definition. The term was first coined in 1998 and it is defined as "the internet of things allows people and things to be connected anytime, anyplace with anything and anyone, ideally using anypath/network and any service"[1]. The ultimate objective of IoT is to create "A better World for human beings" , in which objects around us know what we like, what we want and what we need and hence act accordingly without explicit instructions [2]. Based on the application domain, IoT applications can be classified into five categories such as smart medical services, smart home, smart city, smart environment and smart enterprise. The technological advancements led to an exponential increase in the number of interconnected sensing and computing devices (smart devices). As a consequence, the number of potential threats and possible effects against security or privacy of things or an individual has grown rigorously. For providing a large number of reliable services, designers stumble upon several challenges in particular, in security – related research areas. It is unfortunate that these security needs are not yet well – recognized. Hence it is necessary to study about the security threats and general privacy issues. This survey briefs about IoT security issues and various attacks. More specifically it covers

- Motivation for IoT security
- IoT applications
- IoT security issues in IoT layered architecture
- Existing survey methods for providing security, solutions and their limitations .

II . MOTIVATION FOR IOT SECURITY

IoT security is an trending research area that is attracting the researchers from academic, industrial as well as governmental sectors.. Several organisations worldwide are involved in the design and development of IoT based systems [3]. Attacks on IoT devices are simple and easy to conduct. Silivia et al., showed that an adversary can compromise a home alarm system by eavesdropping on the RF signal used for enabling and disabling the alarm system [5]. Security challenges such as general security, network security and application security in the IoT are discussed in [4].

The international data corporation predicts that more than 200 million devices will be connected to the internet by the year 2020, with a good amount of these being appliances, there will be a large opportunity for hackers to use these devices their advantage through "Denial of Service" attacks, malicious email other harmful Trojans or worms. A recent HP study report says that on commercialized IoT deployments found that 80% of IoT devices violate privacy of personal information such as name, date of birth etc., more than 80% failed to require passwords of sufficient length and complexity and 60% had security vulnerabilities in their user interfaces [6, 7].

III . APPLICATIONS OF IOT

As per the survey conducted by the IoT-I project in 2010 [27] indicated IoT's circumstance applications could be grouped in 14 domain viz; Transportation, Smart home, Smart city, Lifestyle, Retail, Agriculture, Smart factory, Supply chain, Emergency, User Interaction, Healthcare, Culture and tourism, Environment and Energy. Some of them are listed below in table 1 .

TABLE 1. APPLICATIONS OF IoT

SL	Field of Application	Examples of application
1	SMART MEDICAL SERVICES	It includes Monitoring the respiration, body position, activity level, skin temperature, fitness monitoring, calories burned, quality of sleep monitoring , drug delivery systems , early detection of illness , etc.,
2	SMART HOME	○ Sprinkler installed in garden to will detect rain and turn itself off/on for saving energy. ○ Capturing an image from a door camera and sending it to the user when someone rings the door bell. ○ A smart bulb will reacts to the context and can change its colour and brightness according to the user preferences , period/time/day and activity [10] ○ A water bottle that records drinking habits while keeping the users healthy and hydrated [11].
3	SMART CITY	**Smart Traffic Management:** UBER [8] a taxi service allows users to request a ride at any time . The corporation in a particular place sends a cab .In contrast to traditional taxi services, there is no need of either phone call or pickup location. A mobile application shows the cabs close to the users and their movement in real time. **Smart Resource Management:** A Smart waste management enables a sensor- embedded trash can that is capable of real time context analysis and alert the authorities when it is full and needs to be emptied [9].
4	SMART ENVIRONMENT (Energy Management)	✓ Air quality monitoring ✓ Water quality monitoring ✓ Natural disaster monitoring ✓ Smart Farming
		Transportation and Logistics:
5	SMART ENTERPRISE	IoT provides solution to maintain real time shipment tracking . (Example Cantaloupesus [12] allows the user to keep track of stocks in vending machine remotely). **Energy and Production and Resources management :** Smart farming through accommodating increasingly complex and interconnected farming equipment (Example Heatwatch is a cattle monitoring solution that records the activities of each animal [13].

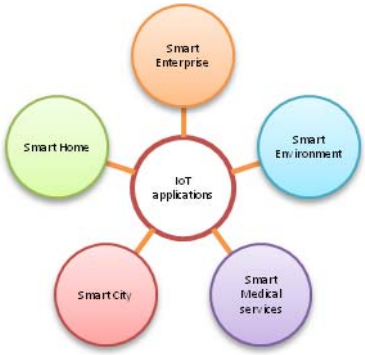

Fig.1. IoT applications

IV . NEED FOR SECURITY IN IoT

In the present internet scenario, enormous number of protocols and technologies are available to address most of the security issues for wireless networks , but still the existing tools have a constraint in applying them in the domain of internet of things (IoT) because of limitations in IoT hardware nodes and WSNs . Another reason is conventional security protocols devour large amounts of memory and computing resources. Also IoT devices usually have to work in harsh, erratic and even intimidating surrounding environments, where they are prone to various security breaches. By 2020, more than 25 billion IoT devices will be in use Table 2, shows the various categories of industries that will be using IoT [26].

TABLE:2 IOT UNITS INSTALLED (CATEGORY WISE)

Category	2014	2015	2020
Automotive	189.6	372.3	3,511.1
Generic Business	479.4	623.9	5,158.6
Vertical Business	836.5	1,009..4	3,164.4
Consumer	2,244.5	2,874.9	13,172.5
Grand Total	3750.0	4,880.6	25,006.6

Any security mechanism should be designed to provide confidentiality, Integrity, authentication and non repudiation. Both IEEE (Institute of Electrical and Electronics Engineers) and IETF(Internet Engineering Task Force) is mainly working towards the design of communication and security issues for communication between IoT and the internet.

V. SECURED IOT ARCHITECTURE

IoT has to ensure the security of all layers. In addition, IoT security should also include the security of entire system crossing the perception layer, network layer , middleware layer and application layer.

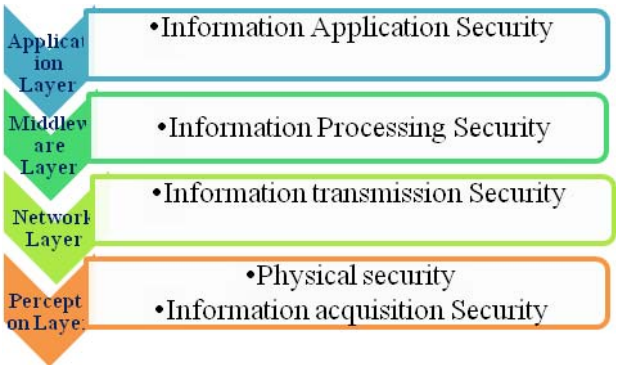

Fig.2. Secured IoT architecture

A. Perception Layer

i.Physical Security Policy

Perception layer is the lowest layer of the IoT. It is accountable for the acquisition of information across the whole IoT network. Perception layer security issues include information acquisition security and physical security of hardware such as sensor devices, RFID nodes, and sensor terminals etc., Implementation of the physical security at the perception layer has to be provided.

a. Sensor network Security Policy

Sensor network technology has constraints such as physical capture of sensor nodes and gateway nodes, integrity and congestion attacks, DoS attacks, eavesdropping and node replication attacks. To construct a security framework for the sensor network , security policies such as encryption algorithms, key distribution policies, intrusion detection mechanisms need to be involved [14]. Tinysec, LEAP protocol are some of the existing security frameworks.

b. RFID security policy

The security issues related to RFID include leakage of location information of RFID tags and users, Sniffing attacks, man-in-middle attacks, cloning, replay and tampering attacks .In major cases RFID security is implemented using physical methods or code mechanisms or sometimes both. Some of the methods of physical security are Data encryption, blogger tag, jamming, kill order policy. Few of the RFID security protocols are LCAP, Hash Lock, Hash Chain, re-encrypt protocol [15].

c. Sensor Terminals security policy

Unauthorized access, theft or damage of confidential information, replication of SIM information, imitation of air interface information are the major security issues related to the terminals of sensors in internet of things (IoT).

ii.*Information Acquisition Security Policy*

Apart from the security issues of the physical security, it is the responsibility of perception layer to handle issues related to information acquisition security. Security issues such as wiretapping, tampering, cheating and replay attacks are some of the possible attacks.

B.Network Layer

a.Information Transmission Security policy

In the architecture of IoT, the major task of network layer (second layer) is to transfer the information across the network, since IoT is implemented on the basic communication framework, it is prone to various attacks including Denial of Service (DoS) attacks, man-in-middle attacks, gateway attacks, storage attacks etc., The security strategy at the network layer need to maintain authenticity, confidentiality, integrity and data availability whenever data is transmitted across the network. Key management, authentication, intrusion detection and negotiation can be implemented to make the network immune against such attacks [16].

C.Middleware Layer

a.Information Processing Security Policy

It is the responsibility of middleware layer for processing information and to provide interface between the network layer and application layer in the IoT layered architecture. Some of the existing technical issues are related to privacy, security and reliability in the middleware layer. Ensuring confidentiality and safe storage makes the middleware layer more secure.

D.Application Layer

a. Information Application Security Policy

Privacy is the major component in the application layer security, access privileges must be limited in order to ensure the unauthorized access and usage of data. Data distortion technology and data encryption technology agents are few technologies upon whom the common privacy protection technologies may be based upon for ensuring privacy of database. In order to achieve data security, data backup and recovery mechanism must be done properly. Some of the data privacy techniques are TLS, SSL, DNS etc.,

TABLE .3 EXISTING METHODS PROVIDING SECURITY AND THEIR LIMITATIONS

Layer/Method/Author	Issues it addresses	Solution	Limitation
Perception Layer / AAL / A.Dohr et al [2]	Safe and secured life style for the elderly people	Keep in Touch (KIT) through smart objects and methodologies like RFID,NFC and CLH(Closed Loop Hierarchy)	This method fails to address security and privacy issues, even though it identifies security, privacy and reliability as the major needs of intended users
Perception layer / Cybersensors / Liu et al.,[18]	Lack of real time data/output from physical objects	Cyber sensors capturing the data from physical objects can be used later to perform actions or real time event response	Few technology for the sensors does not yet exist
Perception Layer / ASM / Reijo M Savola et al [19]	Security threats are identified in data integrity and adapts to environmental and censored changes that it identifies by using the security metrics	ASM method has 4 steps, i.Continuous monitoring ii.Analytics and predictive function. iii.Decision Making iv.Metrics based adaptive security models. Sensors are analysed to gather information about devices surrounding and environment	Major limitation is sensors can fall subject to interference from other electronic devices.another limitation is it do not provide details on the security metrics
Network Layer / Security Middleware / You-Guo and Ming-FU –[25]	To provide security to intelligent home systems and communication devices	It uses entity identification, secure storage, security audit, data encryption/decryption	Middleware is an upcoming trend , it is not yet widely integrated or widely in use
Network Layer / Authentication and access control / Lui et al.,[20]	Fixes loop holes in device security and data integrity	A user requests authentication to access a device, things ask for permission to do so from a "RA-Registration Authority" RA approves/denies the request.	Systems are still very vulnerable to the man-in-middle attacks and eavesdropping attacks.
Application layer / DSM / Jafari et al., [21]	Security metrics for e-health information systems	Five elements are proposed that deals with security analysis and policies	It fails to address the methods for the identification ,collection, computation or the application of the security metrics to address the security issues
Application layer / Game Theory / Cox and Balasingham [22]	Attacks of various varying complex systems	Method of attacking systems to develop better security strategies	Prototyping is not yet released/completed. Hence not clear how the system will handle varying complex systems
Application Layer / ASTM / Abie H [23]	A system that can adapt itself for the environmental changes	Adaptive learning technique by changing the internal parameters and dynamic change to architecture	ASTM model has tp be validated against dynamic scenarios of application domain and unknown threats
Application Layer / CCM / Weiss [24]	A security metric model based on risk assessment approach	In this model the security is quantified in terms of incident asset loss	Availability and attainability of the data is a major challenge to measure all the security metrics

V CONCLUDING REMARKS

The emergence of the IoT paradigm in the last decade has led to various threats and attacks against security or privacy of Internet of Things (IoT). In this paper we have articulated that as more and more IoT applications are developed, it results in the expansion of the surface area for external attacks. We have classified those attacks based on the layers of the IoT architecture and discussed them with possible solutions. Also we have summarized existing methods providing security and their limitations in various layers. In order for the consumer to hold the IoT technologies and applications, these privacy and security issues and limitations need to be addressed and implemented, so that potential of IoT technology can be used for constructive applications. In the end, we believe this survey will serve as an important contribution to the research community , by documenting the present application and security attacks in various layers and motivating young researchers in developing new protocols to address security issues in the perspective of Internet of Things(IoT).

References

[1] C.Perera.,A.Zaslavsky.,P.Christen and D.Georgakopouls : Context aware computing for the internet of things, A Survey, Communications surveys tutorials , IEEE vol 16, No 1 pp 414-454(2013).

[2] A.Dohr ., R.Modre-opsrian ., M.Drobics, D.Hayn.,G.Schreier : The Internet of Things for ambient assisted living , Seventh International Conference on Information Technology ,pp.804-809 (2010).

[3] R.Khan.,S.U Khan., R.Zaheer and S.Khan, : Future of Internet-The internet of things architecture, possible applications and key challenges , in Proc. IEEE 10th International Conference. Frontiers of Information Technology pp.257-260(2012).

[4] H.Ning., H.Liu., and L.Yang :Cyberentity security in the internet of things , computer, vol 46,no.4,pp 46-53 (2013).

[5] S.Cesare : Breaking the security of physical devices, accessed on 07-Nov 2016.

[6] Internet of Things research study, accessed on 20-Oct 2016.

[7] HP White paper retrieved in Aug 2015 http://go.saas.hp.com/food/internet of things

[8] Streetlight Inc : Parksight –The complete smart parking solution, Tech rep (2013).

[9] Smart Belly Components :Big Belly Solar intelligent waste and recycling of collection system, Tech Rep (2013).

[10] Koninklijke Phulips :Meethu Personal wireless lighting , (2013).

[11] OleoApps Inc :Bluefit –Smart water bottle, http://bluefitbottle.com (2013).

[12] Cantaloupe systems : Seed Platform ,http://cantaloupesys.com (2012).

[13] GEA Farm Technologies : Heatwatch including recounter II Technology:Heatwatch ,Tech Rep (2006).

[14] L.Xiao-Wei : Wireless Sensor Network technology,Beijing Institute of Technology press ,pp.241-246 (2007)

[15] Z.Young-Bin and F.Deng-Guo :Design and analysis of cryptographic protocols for RFID, Chinese Journal of computers pp.583-584 (2006).

[16] Q.Gou., L.Yan., Y.Liu and Y.Li :Construction and strategies pm green computing and communications and IEEE Internet of Things and IEEE Cyber ,pp.1129-1132 , (2013).

[17] D.Singh., G.Tripathi., and A.j. Jara : A survey of Internet of Things – Future Vision, architecture, challenges and services, in Proc. IEEE World Forum on Internet of Things pp.287-292 (2014).

[18] Huansheng Ning and Hong Liu.,Laurenct T Yang , Cyberentity security in the internet of Things, Vol 46,No.4 pp.46-53 (April 2013).

[19] Reijo M Savola., Habtamu Abie ., Markus Sihvonen:Towards metrics driven adaptive security management in e-health IoT applications, Proc of the 7th International Conference on Body Area Networks, pp.276-281 (2012).

[20] .Lui., Xiao., Chen : Authentication and access control in the Internet of Things ,32nd International Conference on distributed computing systems workshop (ICDCSW) ,pp.588-592 ,(2012).

[21] . Kozlo et al: Security and Privacy Threats in IoT architectures, Proc of the 7th International Conference on Body Area Networks, pp.256-262 (2012).

[22] Abie H., and Balasingham :RISK based adaptive security for smart IoT in e-health , Proc of the 7th International Conference on Body Area Networks, pp.269-275 (2012).

[23] Abie H., and Balasingham I.: Adaptive security and trust management for autonomic message oriented middleware, IEEE 6th Intl conference on mobile Adhoc and Sensor Networks (MASS'09) pp.810-817 (2009).

[24] Wei B Weissmann O ., and Dressler F., : Comprehensive and comparative metric for information security , in Proc of IFIP – International Conference on Telecommunication security ,modelling and analysis ,pp 1-10 (2005).

[25] Li You Guo., Jiang Ming Fu: The reinforcement of communication security of internet of things , International Symposium on information science and Engineering , pp531-534 (2010).

[26] www.gartner.com accessed on 20.12.2016

[27] Vermesan, O., Friess, P. and Furness, A. (2012) The Internet of Things 2012. By New Horizons.