http://dx.doi.org/10.21172/ijiet.81.017

A Survey on Privacy and Security in Internet of Things

S.Harini
UG Student

K.Jothika,
UG Student

K.Jayashree,
Associate Professor

Abstract - In the last few years, the world has witnessed major growth of everyday devices that are Internet-enabled, a concept commonly referred to as The Internet of Things. Internet of Things and cloud computing together give us the ability to sense, collect, process, and analyze data so we can use them to better understand behaviours, habits, preferences and life patterns of users and lead them to consume resources more efficiently. In such knowledge discovery activities, privacy becomes a significant challenge due to the extremely personal nature of the knowledge that can be derived from the data and the potential risks involved.The real spreading of IoT services requires customized security and privacy levels to be guaranteed. Thus this paper presents a survey on privacy and security issues in Internet of Things.

I.INTRODUCTION

Internet of Things (IoT) is a domain that targets at creating a smart world by linking various physical and virtual devices and enabling an interaction amongst them. IoT works by collecting data from various sources and processes them to provide certain useful information for various serviceswith or without human intervention. The automated information exchange between two devices in IoT, takes place through some specific communication technologies such as Wireless Sensor Networks (WSN) and Radio Frequency Identification (RFID). IoT has numerous applications [3][11] such as the information and communication industry has been impacted by IoT and there has been a transformation through fantastic opportunities brought by IoT. Consumer related activities have seen a major development through IoT. IoT has many potential applications in prevention of natural disasters like earthquake and forest fires, monitoring the conditions and vibrations in buildings and provides warning regarding these. IoT can be used in warning the consumers regarding the expiry date of products,on the presence of any allergic ingredients and other options in accordance to user's preference. IoT can be highly efficient and useful in creating a smart home by monitoring the consumption of water, energy and other resources and to conserve the same. Home security system, signalling the necessity to switch off electrical appliances are some applications offered by IoT , to the home environment. One of the major uses/applications of IoT is in the monitoring the patients in hospitals and old age homes. As far as the environment is concerned, devices that monitor temperature levels in water bodies and the environment can be used in detecting the high levels of global warming [3]. In addition to all the benefits of IoT , it is important to consider the different layers of security and privacy concerns that are to be addressed.[6]

II .BACKGROUND

2.1 PRIVACY

IoT is a technology that can provide many utilities and helpful services to individuals, but due to the usage of personal information, violation of privacy is one of the major problems in IoT. Thus the paradigm of IoT should be such that they express the user's requests for data access. Each domain or system in IoT should have specified privacy policies[4]. The main research focus is on the integrity and authenticity of sensor data as well as privacy of data in sensors. Regulations are required to be set up to preserve privacy of people, as in most cases people are unaware of sensors in their life [14].

In order to ensure information privacy, an individual should be given the following guarantee:

- The privacy risks imposed by smart objects should be known to the user/individual; users should know that they are being sensed.
- The collection and processing of personal information by smart objects should be controlled by individuals; they must be able to choose if they are being sensed or not.
- An individual should be aware and should control the use and dissemination of personal information by the smart things to any entity outside the personal space; users must be able to remain anonymous[1][14].

But the scope or concept of personal sphere will vary from one situation to another and it is a little difficult to determine those that constitute the personal boundary of an individual. Thus while designing new smart systems,care must be taken in order to carefully access the sensitivity of the information and also should adhere to user requirements. Hacking and major system crashes are certain negative impact due to the exposure of personal or confidential information to the third party[1].

2.2 SECURITY

The main objective of IoT security is the safety of various devices and items connected to one another and the safety of network that communicate in. Home automation systems, communication between machines and energy grids act as vulnerability points in IoT and also lead to increased volumes of data [2]. Preserving the confidentiality,availability and integrity of information is referred to as information security. This is a basic requirement of the IoT services for the industrial environment in order to ensure information security for the industry/organisation as well as for the wellness of citizens[5].There are several security concerns in IoT through Back-end of IT systems, Front-end sensors and equipments and Network.

Data received by the front-end sensors and equipments via the built in sensors, is transmitted using M2M devices or modules. The security of machines with business implementation and node connectivity is involved in this process. As these are distributed in the absence of monitoring sensors any intruder can easily access these devices paving the way for illegal actions and damage. Network congestion may happen due to the large number of nodes and groups existing in the IoT[6].
Figure 1 and Figure 2 from paper [11] clearly showcase the various security issues and attacks in WSN and RFID systems. In WSN the main security issues are due to the Denial of Service attacks in Physical layer, Link layer, Network layer, Transport layer and the Application layer.[11]

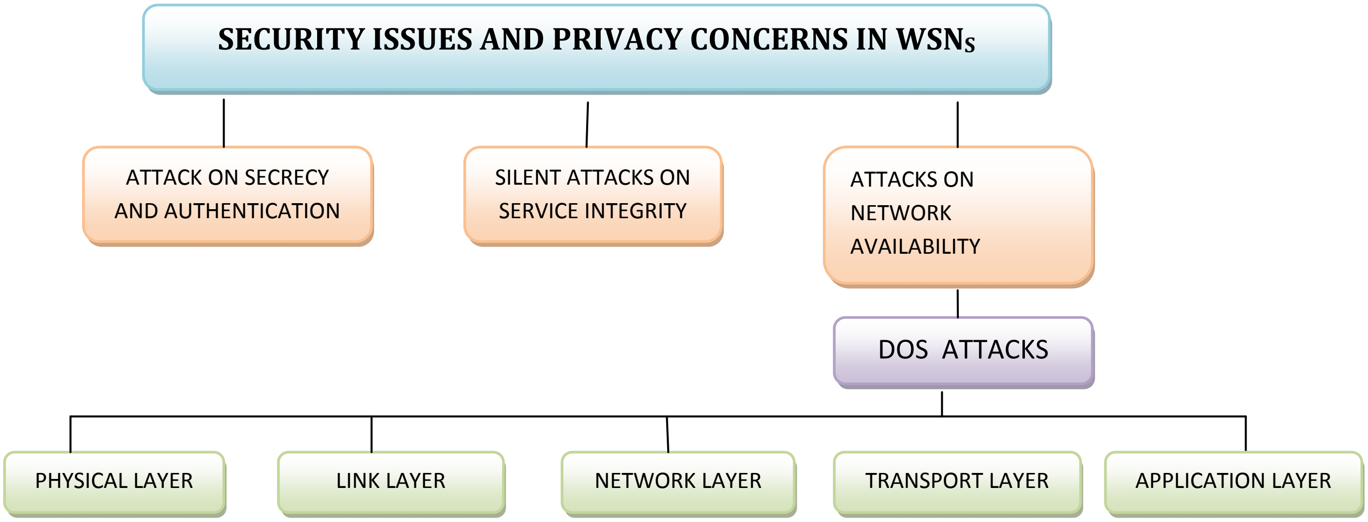
SECURITY ISSUES AND PRIVACY CONCERNS IN WSNs
ATTACK ON SECRECY AND AUTHENTICATION
SILENT ATTACKS ON SERVICE INTEGRITY
ATTACKS ON NETWORK AVAILABILITY
DOS ATTACKS
PHYSICAL LAYER
LINK LAYER
NETWORK LAYER
TRANSPORT LAYER
APPLICATION LAYER

Figure 1 – Hierarchical diagram of security issues in Wireless Sensor Network[11]

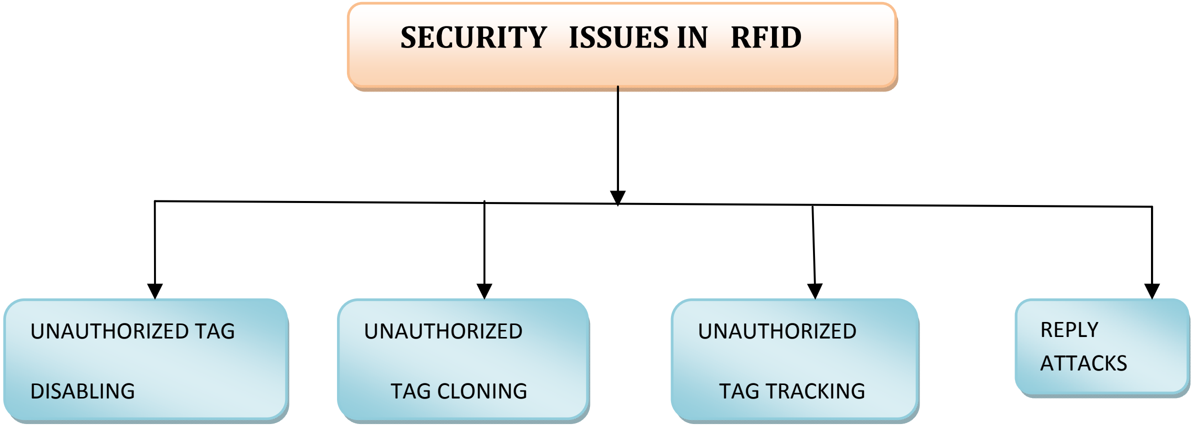

Figure 2 –Security issues in RFID[11]

2.3 DESIGN OF IOT TECHNOLOGIES

The design stage of the IoT applications should take into account the information security and privacy considerations. The heterogeneity of the objects in IoT is a major challenge in implementing the relevant security layers.[2] Acquiring and transmitting poor quality of data by IoT devices due to device calibration, device faults should be avoided. [8] IoT systems should be designed in such a way that they have Self-organisation capabilities. They should be Energy-optimised solutions in order to optimize the use of energy required for communication. Apart from these challenges while building IoT, there are a few others like scalability, Localisation and Tracking capabilities, Heterogeneity of devices.[10]

2.4 SITUATIONAL RISKS

- With increase in the number of individuals, the security and privacy considerations become content aware and hence the complexity in identifying and accessing becomes more.

- When data is used for other purposes than the one specified, the existing challenge becomes more severe to consider. For specified purposes the data collected may be accessed by law enforcement authorities or intelligence agencies and this would lead to violation of data security.
- Several technological safeguards have to be implemented in order to ensure information security. Especially exposure of individuals' information might be used to physically them various ways. Data minimisation,encryption of data such as passwords, ATM pin,control of access and giving individuals an enhanced control over their personal data are some of the safeguard measures that can be implemented.

III. SURVEY

Jan Henrik Ziegeldorf et al[1] has proposed the various threats and challenges to data privacy in the IoT. The authors has specified identification, Localisation and tracking, Profiling , Privacy violating interaction and presentation , Inventory attack and lifecycle transitions as the major threats to data privacy. As a solution, Privacy legislation i.e., recognizing it as a fundamental right in the constitutional law, has been proposed. Also various evolving technologies of IoT , such as RFID technology ,wireless sensor network(WSN) technology and their associated problems have been discussed. In paper [7] Abuse of tags , Personal privacy leak , Reader's risks, Signal interference have been mentioned as some of the security threats in the RFID system . Some solutions to these threats are Tag killing , Tag sleeping , Data coding and data integrity check , Relabeling , Re-encryption and Tag blocking. There is an increased focus on personal information security when it comes to IoT and also the changing landscape of data privacy. This foresees the analytical and integrated capabilities of IoT as next big IoT thing . In order to enable enterprises to become more data and IT driven , there are certain areas of information security that have been highlighted . Also devices or technologies such as RFID tags, NFC sensors , embedded systems in vehicles have been found to generate data in IoT . Security risks have increased with vast number of wearable devices ,embedded appliances . The access of individual information by third party , over which the users have very little control , is a major security issue that has been proposed in various places.[2][7]

JohannnaVirkki and Liquan Chen [3] have explicitly dug deep into the individual privacy concerns in the IoT . The research has been done through interviews in China and Finland to 22 people who are working on the development of IoT . The results reflected that most of them believed, users would be able control their privacy to a certain extent , if not completely; and believe this would improve in next 10 years . Also these researchers suggested that IoT would grow manifold in the near future and an all-round network would come to use. There are research directions for the IoT, advancement in which , would lead to more sophisticated environment , using IoT. Areas of research requirement includes massive scaling that deals with efficient management of number of devices and their operations. Architecture and dependencies associated with these is yet another challenge . Creation of knowledge from millions of raw data is to be performed in such a way that their utility is increased . The robustness of the devices in IoT poses major challenge as the efficiency may not be the same with passage of time. In addition to these openness, security and privacy of data have been published as some of the critical research directions for IoT . These are broadly discussed by John.A.Stankovic [4] ..Privacy concerns in IoT's involve areas like privacy in device , privacy during communication , privacy in storage and privacy at processing.[6] Some of the main security requirements that need to be implemented in IoT are : Network security , Identity management , Privacy , Trust and Resilience. Stored data must not expose undesired properties , such as identity of person and this is Data Privacy ; A single person not being identifiable as a source of data or an action is the property of Anonymity; Anonymity with accountability is what is Pseudonymity ; Specific actions of a same person must not be linked, which is Unlikability;[9]

IV.PROPOSED WORK

4.1 MOTIVATION

This study advances the IoT privacy and security. Also cloud service applications have been motivated by the IoT services. For developing software architecture for privacy and security in IoT solution designs we seek to share a blueprint. Satisfaction of the users of IoT applications is of prime importance and hence it is mandatory to reduce the privacy and security risks in this field.[5]

4.2 DIRECTIONS FOR FUTURE DEVELOPMENT

Developments in computing and the reconfiguration of industry towards the energy positive buildings, smart grid technologies and renewable energies play a key role in the "The Industrial Revolution". IoT has not yet been developed at higher stages. It is still at the early stage. However, in the future there will be more innovation. They are: More research on real life applications ; Greater public understanding and discussion of the technology , its issues and potential benefits needs to be developed . Efficient and scalable encryption protocols/techniques need to be employed in large scale IoT system and devices . In order to protect the devices physically and from attackers , white-box cryptography can be helpful which hide the encryption keys by transforming them into large look-up tables . [2][8]

According to paper [12] security initiatives toward Internet of Things are :

a) **CRYPTOGRAPHY** : This technique is implemented through some algorithms like AES , SHAI , MD5 and RSA etc. Protection towards confidential information that are stored in network , also secure transmission of data over network is achieved through cryptography.

b) **END TO END SECURITY** : TLS/SSL and IPSec are certain protocols that provide end to end security in traditional as well as modern internet . Data integrity is maintained through this.

c) **FIREWALL or IPS** : This has deep packet inspection capability which can be useful in controlling traffic in the way of destination.

A new security system can be designed by making a few changes to the existing IoT architecture.
The IoT architecture usually consists of three layers : Application layer , Perception layer and network layer.
The proposed security architecture requires subdividing these layers resulting in six layers : security application layer , application layer , security network layer , network layer , security perception layer , perception layer . [13]

The differences in the instruction set of ARM processor , used in the IoT devices with respect to other conventionally used processors , is a major challenge that arises . Other areas that require research and concern are , protection at run-time software from memory vulnerabilities. Another critical area lies in communication protection and defence techniques against novel botnet attacks , exploiting IoT devices.[8]

V. CONCLUSION

This survey motivates thedetailed analysis of challenges and privacy threats in the IoT . Privacy violating interactions and presentations , inventory attacks, information linkage and lifecycle transitions are the four major threats that will arise in the future as a result of IoT evolution. This study brings a new perspective in IoT research. Most of the research papers on IoT reflect a fact that the world is moving towards the IoT and that it could be mandatory in the future. This survey paper reflects the necessity to concentrate more on security and privacy aspects and also provide some technical solutions to the handle/control the IoT applications efficiently.[1][3]

REFERENCES

[1] Jan Henrik Ziegeldorf, Oscar Garcia Morchon , Klaus Wehrle – Privacy in the Internet Of Things : Threats and Challenges , Communication and distributed systems , RWTH Aachen University , Aachen , Germany.

[2] Vladlena Benson – Personal information security and the IoT : The changing Landscape Of Data Privacy. Computer communication and collaboration(Vol.3 , Issue 4,2015) ISSN 2292-1028(Print) 2292-1036(Online), Submitted on Nov 21 , 2015.

[3] Johanna Virkki and Liquan Chen – Personal Perspectives : Individual Privacy in the IoT , Advances in Internet Of Things , 2013, 3, 21-26. Published online April 2013 (http://www.scirp.org/journal/ait).

[4] John.A.Stankovic , Life Fellow ,IEEE – Research Directions for the Internet of Things .

[5] Ivor.D.Addo , Sheikh I.Ahmed , Stephen S.Yau , Arun Buduru– Reference Architectures For Privacy Presentation In Cloud – Based IoT Applications , International Journal of Services computing (ISSN 2330-4472) , Vol.2 , No.4 , Oct-Dec 2014.

[6] J.Sathish Kumar and Dhiren R.Patel , "A Survey on Internet of Things : Security and Privacy Issues" , International Journal of Computer Applications(0975 – 8887) , Volume 90-No 11 , March 2014.

[7] Xiao Nie and XiongZhong , "Security in Internet of Things Based on RFID : Issues and Current Countermeasures , ICCSEE 2013

[8] Elisa Bertino , " Data Security and Privacy in IoT" , International conference on Extending Database Technology , ISSN : 2367-2005 March 2016 on OpenProceedings.org.

[9] Emmanouil Vasilomanolakis Jorg Daubert , Manisha Luthra, Vangelis Gazis , Alex Weismaier, Panayotis Kikiras ,"On the Security of Internet of Things Architectures and Systems" , September 2015.

[10] Ashvini Balte Asmita Kashid , Balaji Patil , "Security issues in Internet of Things (IoT): A Survey" , International Journal of Advanced Research in Computer Science and Software Engineering , Volume 5 , Issue 4 , 2015.

[11] TuhinBorgohain , Uday Kumar, Sugata Sanyal , "Survey of Security and Privacy Issues of Internet of Things"

[12] JuhiGupta , Anand Nayyar , Dr.Priya Gupta , "Security and Privacy issues in Internet of Things" , International Journal of Research in Computer Science ,Volume :02 Issue : 04 2015 , ISSN:2349-3828

[13] Omar Said , "Development of an Innovative Internet of Things Security System" , International Journal of Computer Science Issues , Vol. 10 , Issue 6, November 2013 , ISSN(Print) : 1694-0814

[14] HuiSuo , Jiafu Wan, Caifeng Zou ,Jianqi Liu , "Security in the Internet of things : A Review" , 2012 International Conference on Computer Science and Electronics Engineering(ICCSEE.2012.373).