Scientific Journal Impact Factor (SJIF) : 1.711

IJMTER

International Journal of Modern Trends in Engineering and Research

ISSN (ONLINE) : 2349 - 9745

ISSN (PRINT) : 2393 - 8161

An Overview of Security Issues in Internet of Things

Sudhir Dakey[1], N Kavitha[2], Sneha Dakey[3]

[1,2]Faculty, Department of E.C.E., M.V.S.R. Engineering College

[3]Student, Department of Business Adm.,M.V.S.R. Engineering College

Abstract— The terminology Internet of Things (IoT) refers to a future where every day physical objects are connected by the Internet in one form or the other, but outside the traditional desktop realm. The successful emergence of the IoT vision, however, will require computing to extend past traditional scenarios involving portables and smart-phones to the connection of everyday physical objects and the integration of intelligence with the environment. Subsequently, this will lead to the development of new computing features and challenges. The main purpose of this paper, therefore, is to present and overview of weaknesses that will come about, as the IoT becomes reality with the connection of more and more physical objects. In the distributed form of architecture in IoT, attackers could hijack unsecured network devices converting them into bots to attack third parties. Moreover, attackers could target communication channels and extract data from the information flow. Finally, various layers in IoT architecture are also found to be vulnerable to DoS attacks.

Keywords— Internet of Things (IoT), Security issues, Wireless Sensor Networks (WSNs), Radio Frequency Identification (RFID), DoS Attacks

I. INTRODUCTION

IoT can be defined as a future where every day physical objects are connected by the Internet in one form or the other, but outside the traditional desktop realm. To meet this challenge, it is expected that sensor network and RFID technologies will become increasingly integral to the human environment, in which communication and information systems will be invisibly embedded. Subsequently, massive volumes of data will need to be processed, stored, and presented in an easily interpretable, efficient, and seamless form. Some evidences of the evolution towards ubiquitous communications and information networks can be seen in the growing presence of 4G-LTE and WiFi. The successful emergence of the IoT vision, however, will require computing to extend past traditional scenarios involving portables and smart-phones to the connection of everyday physical objects and the integration of intelligence with the environment. Currently, the Internet is no longer only be accessible from smart-phones and laptops but is a part of such objects as cars, ovens, baby monitors, and TV sets. In addition, the IoT will become completely integrated into medical and other critical devices and pervade majority of sectors. Unfortunately, as with other major developments in the Internet era, growth in the IoT technology will be equally matched by growth in security and privacy concerns. Several researchers are pointing towards the evolving nature of challenges and vulnerabilities in various existing IoT devices. This research paper seeks to investigate the security issues facing the new and dynamic realm of the IoT. The study is organized into five sections. The following section gives technologies used to establish connectivity among various IoT devices. In section III, we discussed how emergent IoT technologies can be used in societies. We have presented proposed plans of India, as an example. Section IV presents all the security issues in IoT. Finally, Section V presents the conclusion.

II. CONNECTIVITY TECHNOLOGIES AMONG IoT DEVICES

The automatic exchange of information between two devices takes place through some specific communication technologies in IoT, which are described below.

A. Wireless Sensor Networks (WSN)

The Wireless Sensor Networks are compositions of independent nodes whose wireless communication takes place over limited frequency and bandwidth. The communicating nodes of a typical wireless sensor network consist of:

Sensor, Microcontroller, Memory, Radio Transceiver, Battery

The required data is collected by the wireless sensors through collaboration amongst the various nodes and is sent to the sink node for directed routing towards the base station. The communication network formed dynamically by the use of wireless radio transceivers facilitates data transmission between nodes.

B. Radio Frequency Identification (RFID)

RFID tags use radio frequency waves for interacting and exchanging information between one another with no requirement for alignment in the same line of sight or physical contact. It uses the wireless technology of Automatic Identification and Data Capture.

A RFID is made up of the following two components:

1. RFID tags (Transponders): The RFID tag is a microchip which contains an antenna, and memory units, which houses a unique identifier known as Electronic Product Code (EPC). The function of the EPC in each tag is to provide a universal numerical data by which a particular tag is recognized universally.

The types of RFID tags are:

Active tag: This type of tag houses a battery internally, which facilitates the interaction of its unique EPC with its surrounding EPCs remotely from a limited distance.

Passive tag: In this type of tag, the information relay of its EPC occurs only by its activation by a transceiver from a predefined range of the tag. The lack of an internal battery in the passive tags is substituted by its utilization of the electromagnetic signal emitted by a tag reader through inductive coupling as a source of energy.

A RFID tag operates in conjunction with a tag reader, the EPC of the former being the identifying signature of a particular tag under the scan of the latter.

2. RFID readers (Transceivers): The RFID reader functions as the identification detector of each tag by its interaction with the EPC of the tag under its scan.

III. INTERNET OF THINGS IN INDIA

According to [4], the vision of INDIA is to develop connected, secure and smart IoT based system for the countries Economy, Society, Environment and global needs. The objectives are:

i. To create an IoT industry in India of USD 15 billion by 2020. This will also lead to increase in the connected devices from around 200 million to over 2.7 billion by 2020. As per Gartner Report the total revenue generated from IoT industry would be USD 300 billion and the connected devices would be 27 billion by 2020 globally. It has been assumed that India would have a share of 5-6% of global IoT industry.

ii. To undertake capacity development (Human & Technology) for IoT specific skill-sets for domestic and international markets.

iii. To undertake Research & development for all the assisting technologies.

iv. To develop IoT products specific to Indian needs in the domains of agriculture, health, water quality, natural disasters, transportation, security, automobile, supply chain management, smart cities, automated metering and monitoring of utilities, waste management, Oil & Gas) etc.

The Indian Government's has planned for developing 100 cities into smart cities in the country, for which Rs. 7,060 crores has been allocated [4]. Also, the launch of the Digital India Program of the Government, which aims at transforming India into digital empowered society and knowledge economy, will provide the required impetus for development of the IoT industry in the country. The various initiatives proposed to be taken under the Smart City concept and the Digital India Program to setup Digital Infrastructure in the country would help boost the IoT industry. IoT will be critical in making these cities smarter. Some of the key aspects of a smart city will be:

- Smart parking
- Intelligent Transport System
- Smart urban lighting
- Waste management
- Smart city maintenance
- Tele-care
- Citizen safety
- Smart Grid
- Smart Energy
- Water Management

Among other things, IoT can help automate solutions to problems faced by various industries like agriculture, health services, energy, security, disaster management etc. through remotely connected devices.

A. Proposed Development Plans

To develop domain specific strategies for IoT including green building, smart grid, smart manufacturing, industrial monitoring, agriculture, smart cities, healthcare, connected homes, telematics and supply chain, safety and security, forest and wild life, automotive, natural disasters, etc.

1) Smart City*:*

To develop tools for and set-up a Smart city model which would include deployment and display of IoT concepts to be used in development of Smart City. The model should cover the concepts like, Smart Lighting, Smart traffic management, Smart building, Smart Health, Smart parking, Wi-Fi Internet access & City Surveillance, Solid Waste Management, Smart Metering, Water Quality, Water Clogging Management in cities, etc.

2) Smart Water :

i. To setup Potable water monitoring tools to monitor the quality of tap water in all government owned education institutes and public places.
ii. To setup project for real-time detection of leakages and wastes of factories in rivers and other natural water bodies.
iii. To setup project for monitoring of water level variations in rivers, dams and reservoirs, for proactive disaster management.

3) Smart Environment:

i. To setup project for alarm and control of CO_2 emissions of factories, pollution emitted by cars and toxic gases generated.
ii. To setup projects to create alarms based on distributed control in specific places like buildings, bridges, and establish a National Advance Disaster Alarm System

4) Smart Health (Remote):

i. To setup projects for monitoring various vital parameters of patients like subtle changes in pulse,

respiration, heart condition, temperature and preventive warning on early onset of pneumonia (in small children) or other life-threatening problems, inside hospitals and at remote patient location including old people's home and ambulance.
ii. To setup projects to detect & provide support to old age persons in case of fall.

5) Smart Waste Management:
To assist the SWACH BHARAT initiative, projects may be setup to create products which are solar-powered trash receptacle and trash compactor that alerts sanitation crews of municipal authorities, when it is full.

6) Smart Agriculture:
i. To setup project for precision farming which uses data analysis to customize operations. The project may include monitoring of soil moisture, vibrations, earth density and pests to detect dangerous patterns in land conditions and create an online update mechanism for farmers.
ii. To setup a project to allow farmers to monitor online, the temperature of grain bins and receive an alert if the temperature rises outside of an acceptable range to help them preserve grains in storage areas. This also can be extended to alerts for pest controls requirements.
iii. To create unmanned tools for spray of pest control and other insecticides.

7) Smart Safety:
i. To setup project to build wearable devices for women, child, old people and physically disabled persons safety.
ii. To setup projects for supporting dementia and other men- tally unhealthy patients from getting lost.
iii. To create low cost tools for intercepting abnormal activities at any location. This can be extended as a solution to provide safety at secluded, remote and border locations.

8) Smart Supply Chain & Logistics:
i. To setup a project for enabling universal ambulance service at any place using any kind of device.
ii. To enable logistics chain managed by government for essential food items to ensuring need-based re-filling and reduction in wastage of food items.
iii. To create tools which could enable faster fulfillment of ecommerce purchases.

9) Smart Manufacturing & Industrial IoT:
i. To setup projects using IoT for planning preventive and in-time main- tenance for equipments in various manufacturing verticals. The sensors for early defect detection will help in reducing equipment malfunction and hence downtime.
ii. To setup projects for process improvement in manufacturing leading to optimal utilization of resources(fuel, power, as the case may be).
iii. To setup projects for monitoring operations and creating warning/alerts for deviation/damages. For example fire, gas leakage sensors together with alerts.

IV. SECURITY ISSUES AND PRIVACY CONCERNS

The IoT has immense potential for developing the country, as can be understood for the massive development plan laid down by INDIA from section above. But, the whole communication infrastructure of the IoT is flawed from the security standpoint and is susceptible to loss of privacy for the end users. Some of the most prominent security issues plaguing the entire developing IoT system arise out of the security issues present in the technologies used in IoT for information relay from one device to another. As such some of the prominent security issues stemming out from the communication technology are the following:

A. Security issues in the wireless sensor networks (WSNs):

The hierarchical relationship of the various security issues plaguing the wireless sensor network is shown in Figure 1.

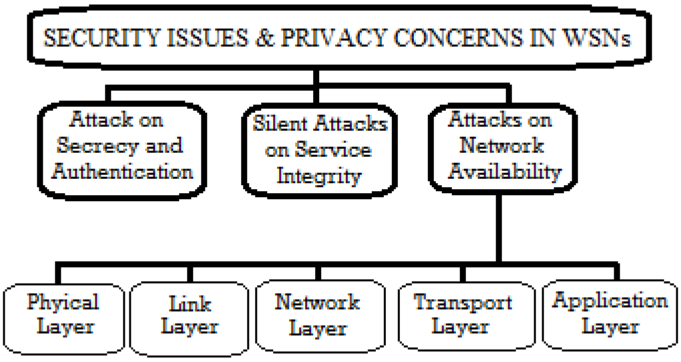
SECURITY ISSUES & PRIVACY CONCERNS IN WSNs
Attack on Secrecy and Authentication
Silent Attacks on Service Integrity
Attacks on Network Availability
Phyical Layer
Link Layer
Network Layer
Transport Layer
Application Layer

Figure 1: Hierarchical diagram of security issues in WSNs

The oppressive operations that can be performed in a wireless sensor network can be categorized under three categories [1]:

i. Attacks on secrecy and authentication

ii. Silent attacks on service integrity

iii. Attacks on network availability: The denial of service (DoS) attack falls under this category. This prevention of accessibility of information to legitimateness by unknown third party intruders can take place on different layers of a network.

B. DoS attack on the physical layer:

The physical layer of a wireless sensor network carries out the function of selection and generation of carrier frequency, modulation and demodulation, encryption and decryption, transmission and reception of data. This layer is attacked mainly through

i. Jamming: In this type of DoS attack occupies the communication channel between the nodes thus preventing them from communicating with each other.

ii. Node tampering: Physical tampering of the node to extract sensitive information is known as node tampering.

C. DoS attack on the link layer:

The link layer of WSN multiplexes the various data streams provides detection of data frame, MAC and error control. Moreover the link layer ensures point-point or point-multipoint reliability. The DoS attacks taking place in this layer are:

i. Collision: This type of DoS attack can be initiated when two nodes simultaneously transmit packets of data on the same frequency channel. The collision of data packets results in small changes in the packet results in identification of the packet as a mismatch at the receiving end. This leads to discard of the affected data packet for re-transmission.

ii. Unfairness: It is a repeated collision based attack. It can also be referred to as exhaustion based attacks.

iii. Battery Exhaustion: This type of DoS attack causes un- usually high traffic in a channel making its accessibility very limited to the nodes. Such a disruption in the channel is caused by a large number of requests (Request to Send) and transmissions over the channel.

D. DoS attack on the network layer:

The main function of the network layer of WSN is routing. The specific DoS attacks taking place in this layer are:

i. Spoofing, replaying and misdirection of traffic.

ii. Hello flood attack: This attack causes high traffic in channels by congesting the channel with an

unusually high number of useless messages. Here a single malicious node sends a useless message which is then replayed by the attacker to create a high traffic.
iii. Homing: In case of homing attack, a search is made in the traffic for cluster heads and key managers which have the capability to shut down the entire network.
iv. Selective forwarding: As the name suggests, in selective forwarding, a compromised node only sends a selected few nodes instead of all the nodes. This selection of the nodes is done on the basis of the requirement of the attacker to achieve his malicious objective and thus such nodes do not forward packets of data.
v. Sybil: In a Sybil attack, the attacker replicates a single node and presents it with multiple identities to the other nodes.
vi. Wormhole: This DoS attack causes relocation of bits of data from its original position in the network. This relocation of data packet is carried out through tunnelling of bits of data over a link of low latency.
vii. Acknowledgement flooding: Acknowledgements are re- quired at times in sensor networks when routing algorithms are used. In this DoS attack, a malicious node spoofs the Acknowledgements providing false information to the destined neighboring nodes.

E. DoS attack on the transport layer:

This layer of the WSN architecture provides reliability of data transmission and avoids congestion resulting from high traffic in the routers. The DoS attacks in this layer are:
i. Flooding: It refers to deliberate congestion of communication channels through relay of unnecessary messages and high traffic.
ii. De-synchronization: In de-synchronization attack, fake mes- sages are created at one or both endpoints requesting retrans- missions for correction of non-existent error. This results in loss of energy in one or both the end-points in carrying out the spoofed instructions.

F. DoS attack on the application layer:

The application layer of WSN carries out the responsibility of traffic management. It also acts as the provider of software for different applications which carries out the translation of data into a comprehensible form or helps in collection of information by sending queries. In this layer, a path-based DoS attack is initiated by stimulating the sensor nodes to create a huge traffic in the route towards the base station. Figure 2 shows all the above mentioned DoS attacks in the different layers of a wireless sensor network.

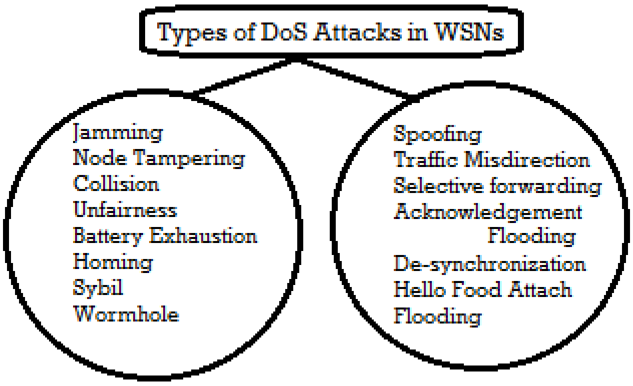

Figure 2: Types of Denial of Attack in Wireless Sensor Network

Some additional DoS attacks are as follows :

i. Neglect and Greed Attack
ii. Interrogation
iii. Black Holes

iv. Node Subversion
v. Node malfunction
vi. Node Outage
vii. Passive Information Gathering
viii. False Node
ix. Message Corruption

Some of the other security and privacy issues in a WSN are:

i. Data Confidentiality
ii. Data Integrity
iii. Data Authentication
iv. Data Freshness
v. Availability
vi. Self-Organization
vii. Time Synchronization
viii. Secure Localization
ix. Flexibility
x. Robustness and Survivability

According to [3], the threats looming over WSN can further be classified as follows:

i. External versus internal attacks
ii. Passive versus active attacks
iii. Mote-class versus laptop-class attacks

According to [2], the attacks on WSN can be classified as:

i. Interruption
ii. Interception
iii. Modification
iv. Fabrication

The attacks on WSN can further be classified as:

i. Host-based attacks
ii. Network-based attacks

G. Security issues in RFID technology:

In context to IoT, RFID technology is mainly used as RFID tags for automated exchange of information without any manual involvement. But the RFID tags are prone to various attacks from outside due to the flawed security status of the RFID technology. The four most common types of attacks and security issues of RFID tags are as follows:

i. Unauthorized tag disabling (Attack on authenticity): The DoS attacks in the RFID technology leads to incapacitation of the RFID tags temporarily or permanently. Such attacks render a RFID tag to malfunction and misbehave under the scan of a tag reader, its EPC giving misinformation against the unique numerical combination identity assigned to it. These DoS attacks can be done remotely, allowing the attacker to manipulate the tag behavior from a distance.

ii. Unauthorized tag cloning (Attack on integrity): The cap- turing of the identification information (like its EPC) esp. through the manipulation of the tags by rogue readers falls under this category. Once the identification information of a tag is compromised, replication of the tag (cloning) is made possible which can be used to bypass counterfeit security measures as well as introducing new vulnerabilities in any industry using RFID tags automatic verification steps.

iii. Unauthorized tag tracking (Attack on confidentiality): A tag can be traced through rogue readers, which may result in giving up of sensitive information like a persons address. Thus from a consumers viewpoint, buying a product having an RFID tag guarantees them no confidentiality regarding the purchase of their chase and in fact endangers their privacy.

iv. Replay attacks (Attack on availability): In this type of impersonation attacks the attacker uses a tags response to a rogue readers challenge to impersonate the tag. In replay attacks, the communicating signal between the reader and the tag is intercepted, recorded and replayed upon the receipt of any query from the reader at a later time, thus faking the availability of the tag. Besides this category, some prominent security vulnerabilities of RFID technologies are [5]:

i. Reverse Engineering
ii. Power Analysis
iii. Eavesdropping
iv. Man-in-the-middle attack
v. Denial of Service (DoS)
vi. Spoofing
vii. Viruses
viii. Tracking
ix. Killing Tag Approach

H. Security issues in health-related technologies built upon the concept of IoT:

Advances and convergence of engineering with biology has paved the way for wearable health monitoring devices which can constantly stream and share the information from the sensor of the health monitor with other devices and social network over the internet. The implementation of automatic collection of data by the sensors and uploading it to the various social networks through a web server introduces some high vulnerability in the whole data transmission process from the monitor to the Internet. Following are the main security vulnerability in health monitoring devices working in synchronization with the Internet:

i. Clear text login information: During login to the account linked with the health monitoring device, the authenticated password of the user is registered in the web server in clear text which is then recorded in log files. This gives way to loss of secured login by making the password available easily through the log files.

ii. Clear text HTTP data processing: The sensor data is sent to the web servers as plain HTTP instructions with no additional security or encryption. Such unprotected HTTP instructions can be easily intercepted for gaining access to various functions of a user account linked to the health monitoring device. From the above mentioned vulnerabilities it is clear that the security measures implemented in the health-related technologies which are socially connected over the internet lack the proper measures to address all the privacy concerns of the end users and puts the users at risk of exposing valuable information about their health to unknown personnel with malicious intents.

Based on the above mentioned security flaws, many other security and privacy issues present themselves in the field of Internet of Things. A few of them are:

i. Theft of sensitive information like bank password.
ii. Easy accessibility to personal details likes contact address, contact number etc.
iii. It may lead to open access to confidential information like financial status of an institution.
iv. An attack on any one device may compromise the integrity of all the other connected devices. Thus the inter-connectivity has a huge drawback as a single security failure can disrupt an entire network of devices.
v. The reliance on the Internet makes the entire IoT architecture susceptible to virus attack, worm attack and most of the other security drawbacks that comes with any Internet connected computing device etc.

V. CONCLUSION

In this paper, an overview of various security flaws in IoT are presented which may prove to be very detrimental in the development and implementation of IoT in the different fields. Security measures such as intrusion detection systems and cryptographic and stenographic security measures are to be adopted to counter the flaws and build more robust infrastructure. In conclusion, we would like to suggest that while going for further development of new implementation methods of IoT, more effort should be made on development of secured measures for the existing as well as new IoT infrastructure.

REFERENCES

[1] Aashima Singla, Ratika Sachdeva, Review on Security Issues and At- tacks in Wireless Sensor Networks, in *International Journal of Advanced Research in Computer Science and Software Engineering*, Volume 3, Issue 4, April 2013, ISSN: 2277 128X.

[2] Xiangqian Chen, Kia Makki, Kang Yen, Niki Pissinou, Sensor network security: a survey, in *IEEE Communications Surveys and Tutorials* 01/2009; 11:52-73. DOI: 10.1109/SURV.2009.090205

[3] C. Karlof and D. Wagner, Secure Routing in Sensor Networks: Attacks and Countermeasures, in *Elseviers AdHoc Networks Journal, Special Issue on Sensor Network (SNPA)*, (2003) September, pp. 293-315.

[4] Draft Policy on Internet of Things, *Department of Electronics & Infor- mation Technology(DeitY)Ministry of Communication and Information Technology Government of India*

[5] Xiao, Qinghan, Thomas Gibbons, and Herv Lebrun, ”RFID Technology, Security Vulnerabilities, and Countermeasures.” *Supply Chain the Way to Flat Organization*, Publisher-Intech (2009): 357-382

[6] Tuhin Borgohain, Uday Kumar, Sugata Sanyal, ”Survey of Security and Privacy Issues of Internet of Things,”

[7] Shen, Guicheng, and Bingwu Liu. ”The visions, technologies, appli- cations and security issues of Internet of Things.” *E-Business and E- Government (ICEE)*, 2011 International Conference on. IEEE, 2011.

[8] Chen Qiang, Guang-ri Quan, Bai Yu and Liu Yang, ”Research on Security Issues of the Internet of Things,” in *International Journal of Future Generation Communication and Networking* Vol.6, No.6 (2013), pp.1-10

[9] Akyildiz,Weilian Su, Sankarasubramaniam Y, Cayirci E, ”A survey on sensor networks,” in *Communications magazine, IEEE* 40.8 (2002): 102-114.

[10] Sen, Jaydip. ”Security and privacy challenges in cognitive wireless sensor networks,” arXiv preprint arXiv: 1302.2253 (2013).

[11] Ahmad Abed Alhameed Alkhatib, and Gurvinder Singh Baicher, ”Wire- less sensor network architecture,” in *International conference on com- puter networks and communication systems (CNCS 2012)* IPCSIT. Vol. 35. 2012, pp. 11-15.