IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Internet Of Things: An Analysis Of Risks To Security And Privacy

Mr. Vijay Jangid

Research Scholar

Department of computer science

Apex University, Jaipur, Rajasthan, India

Dr. Reena Singh

Head of Department & Associate Professor

Department of computer science

Apex University, Jaipur, Rajasthan, India

Abstract

Currently, the global landscape is being shaped by the advent of novel and developing technologies. Consequently, we are encompassed by a multitude of intelligent gadgets. These intelligent gadgets enhance the ease and convenience of our lives. However, we are susceptible to many risks including cyber assaults. Our privacy is always under risk. This study examines the many uses of Internet of Things (IoT) and the associated security risks.

Keywords: -IOT, Sensors, RFID, WSN, Security, Privacy, Internet Introduction

INTRODUCTION

The Internet of Things (IoT) is critical to the future of the internet. The Internet of Things (IoT) is characterized by a global network architecture, whereby every physical object linked to the internet has a unique identity and may interact with other internet-connected objects. Devices such as tablets, laptops, smartphones, and washing machines are examples of gadgets. The Internet of Things (IoT) is a massive network of interconnected objects or gadgets. The gadgets have a microchip that serves as a network connector for all the devices. These microchips collect environmental data and transmit it to both the network and the particular user. One advantage of the Internet of Things (IoT) is the capacity to interact with and access any physical object over the internet. Since internet services are now economically priced, there has been a noticeable increase in the number of devices linked to the internet. In 2008, there were more internet-connected gadgets than humans on the earth. 4.48 billion devices are already connected to the internet, and by 2023, that number is predicted to rise by 40%, according to a research group. By 2025, estimates indicate that there will be 80 billion people on the planet. It is not difficult for attackers to get these devices.

APPLICATIONS OF IOT

Nearly every aspect of our life is connected to the Internet of Things.
The following are a few of them:

A. Environmental Observation

Sensors are used to preserve the environment, and atmospheric factors like water and air quality are continuously monitored. Animals are observed in order to determine their habitats. Our ecology is preserved via the development of more efficient techniques based on the results of the monitoring process.

B. Infrastructure management
One of the most well-known uses is the procedure for keeping an eye on and managing the functioning of infrastructure, such as highways, bridges, train lines, etc. IOT infrastructure management may keep an eye on changes in structural conditions since they have the potential to undermine safety and raise risk. The level of assistance may be raised.

C. Manufacturing
Manufacturing may be optimized in real time. Sensors and control systems can effectively manage the production and supply. This also results in the fast production of novel goods.

D. Home Automation
An automated system may transmit the information about gas, water, and electricity to the respective utility provider. This procedure has the potential to optimize the use of resources. Home automation involves controlling various items such as washing machines, air conditioners, windows, doors, lights, and refrigerators in order to achieve optimum.

E. Transportation
The use of Internet of Things (IoT) technology was first introduced in this particular industry. The system utilizes the combination of photodetectors, Global Positioning System (GPS), and Global System for Mobile Communications (GSM). The car may function as an autonomous unit and establish communication with both other vehicles and roadside infrastructure. The sensors installed in automobiles serve several purposes, including accident avoidance, traffic management, and facilitating parking spot availability.

F. Health and medical systems

It is a very prospective field within the realm of Internet of Things (IoT) technology. Medical equipment may communicate the patient's critical parameters to a secure cloud platform for storage and analysis. Specialized care may be provided to elderly individuals and people with chronic diseases.

INTERNET OF THINGS COMMUNICATION MODELS

The operational aspect of IoT devices is crucial, since it determines how these devices establish connections and interact. The communication models are classified into four distinct categories as follows:

A. Interaction between Devices

In this paradigm, a direct connection is made between two or more devices, establishing communication. No There is a middle application server utilized. Devices connected to the Internet of Things (IoT) may exchange data over a variety of network protocols. These are often connected by means of Bluetooth or Zigbee technologies. Every device in a device-to-device network follows a set protocol for message exchange and communication. Data transmission via home automation systems is bandwidth-limited. IOT devices like light switches, door locks, and lightbulbs often communicate over low bandwidth in home automation systems.

Fig.1. Interaction between Devices

B. Device to Cloud Interaction

This tactic makes use of an application service provider or other internet cloud service to enable data exchange and communication. Wi-Fi or Ethernet are the two ways the device connects to the IP network. Large companies use this kind of communication strategy, like Samsung SmartTV. Data about user viewing is sent to Samsung for analysis at this location via the Internet connection. By enhancing the device's functionality, this method offers the user more value.

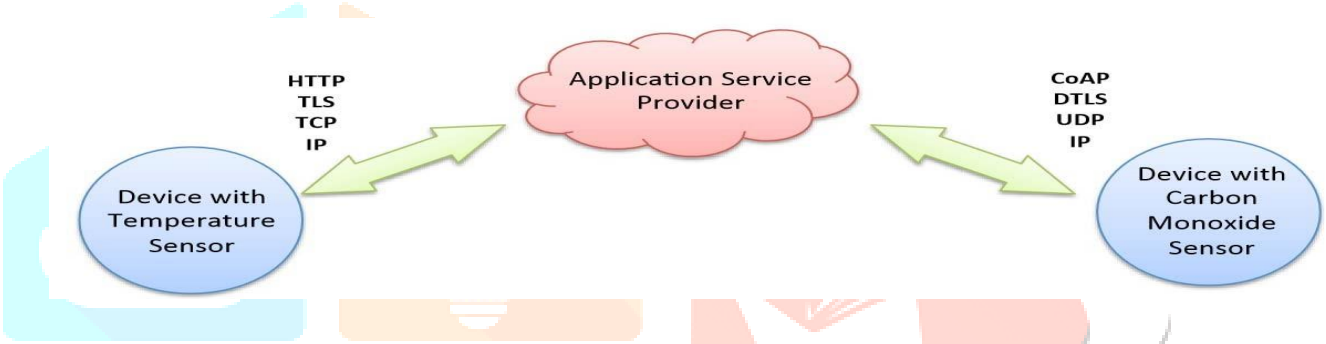

Fig.2. Device to Cloud Interaction

C. Device model for the gateway

An application layer gateway (ALG) service connects the Internet of Things devices in this paradigm to the cloud service. Here, the application serves as a go-between for the cloud service and the device. It uses a local gateway device for more rapid and secure data conversion. Installed mobile apps often act as local gateways for cloud service data transfer and device connectivity. It is not possible to have direct communication between fitness trackers and cloud services. Thus, they depend on applications for smartphones to upload the data to the cloud.

Fig.3. Device model for the gateway

D. Model for exchanging back-end data

Users may more easily export and evaluate data about smart objects from several sources, including cloud services, thanks to this model's communication architecture. After then, the data is sent to further application service providers. Data gathering and analysis are greatly facilitated by the design. To keep track of the plant's energy use, an industrialist would be very interested in gathering data from Internet of Things (IoT) devices and utility systems. The back-end data sharing allows us to view and evaluate the data.

Fig.4. Model for exchanging back-end data

SECURITY REQUIREMENTS

Technologies are advancing swiftly, and as a result, machines are also progressing at a fast pace. The advancement of technology has resulted in several risks and concerns about privacy. The intelligent gadgets will establish communication and share data with one another inside a network. If any device becomes infected, it poses a significant danger to the whole system. For instance, in the event of a machine being compromised by hacking, both the manufacturing process and the critical data associated with it may be jeopardized. Several primary security problems include:

A. The accuracy of the data

The precision of the data sent between two nodes is a crucial concern. Therefore, it is important to maintain the precision of the data. For instance, in a manufacturing company, if a hacker issues a command to stop production, it becomes a very significant problem.

B. Data secrecy

The data sent between two nodes should be kept secret. Only the sender and recipient should have access to the data, with no other parties allowed. For instance, in the event of a breach of the infrastructure data, there is potential for significant damage to the roads and bridges, as well as a heightened danger to security.

C. Authenticity of Data

Authentication is a procedure that guarantees the integrity and reliability of received data. In the medical and health care system, the patient's parameters are sent to various medical facilities. If a hacker manipulates this data and it is subsequently received, there is a potential danger to the care of the patient.

D. Availability of Data

The accessibility of data to consumers is always a primary problem in the realm of IoT. If the user is unable to access the data, it becomes a significant problem. It should be corrected promptly.

CYBERSECURITY RISKS AND IOT TECHNOLOGIES.

A. Network of Wireless Sensors

Actuators, or processing units, and several sensor nodes, or tiny cells, make up Wireless Sensor Networks (WSNs). The main components of sensor nodes are those for data processing, communication, and sensing. Wireless Sensor Networks (WSNs) are used by the Internet of Things (IoT) for many different applications, including healthcare systems, military applications, logistics, environment observation and forecasting, and habitat monitoring. Attacks may be launched against wireless sensor networks (WSNs) because of the broadcast nature of the transmission channel.

The primary hazards to Wireless Sensor Networks (WSNs) include:

1. Physical Attacks

In order to fully use their capabilities, all objects need be equipped with sensors. Preventing unwanted physical access is a challenging task. An individual with hacking skills has the ability to modify the data of a node or sensor, which might potentially jeopardize the operation of the whole sensor network.

2. Replication of Nodes

This attack involves the replication of an already existing node ID onto a sensor network. Node packet duplication may lead to misrouting, erroneous sensor readings, or network termination. Consequently, the performance of a sensor network is interrupted.

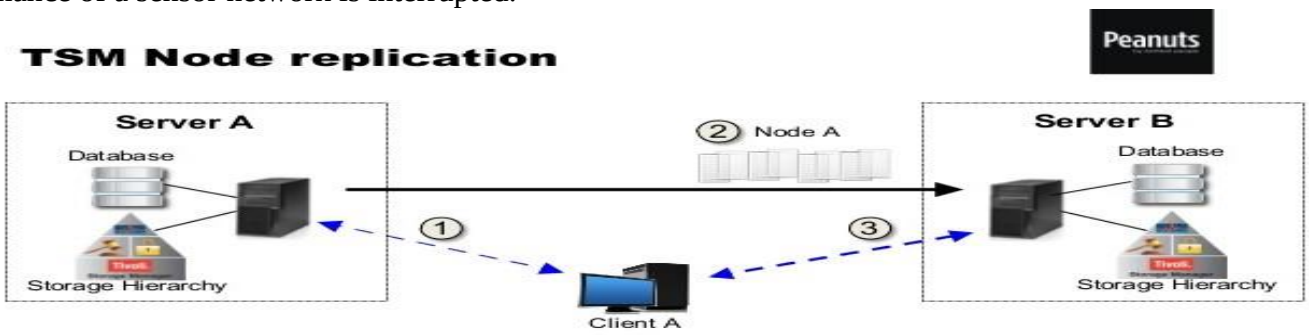

Fig. 5. Replication of Nodes

3. Handpicked Transmission

This attack involves the replication of an already existing node ID onto a sensor network. Node packet duplication may lead to misrouting, erroneous sensor readings, or network termination. Consequently, the performance of a sensor network is interrupted.

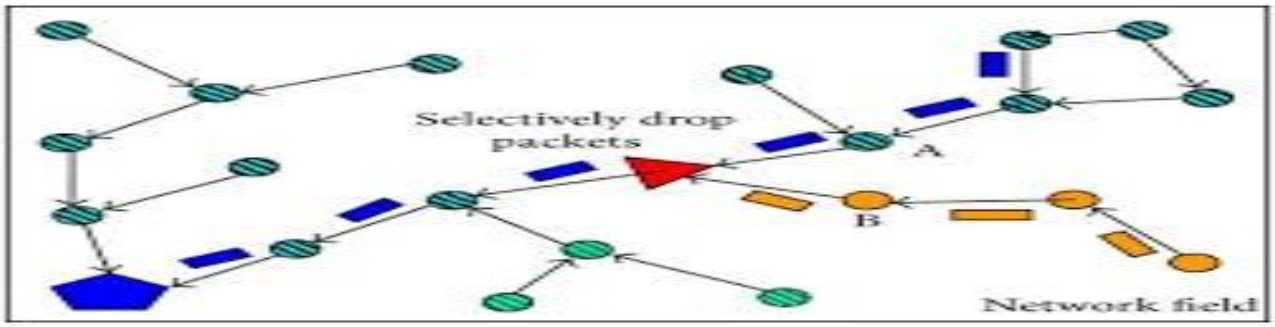

Fig. 6. Handpicked Transmission

4. Attack via a Wormhole

A significant attack known as packet capture occurs when packets are intercepted at one site inside a network and then replayed at a different location. This procedure may be executed in a targeted manner.

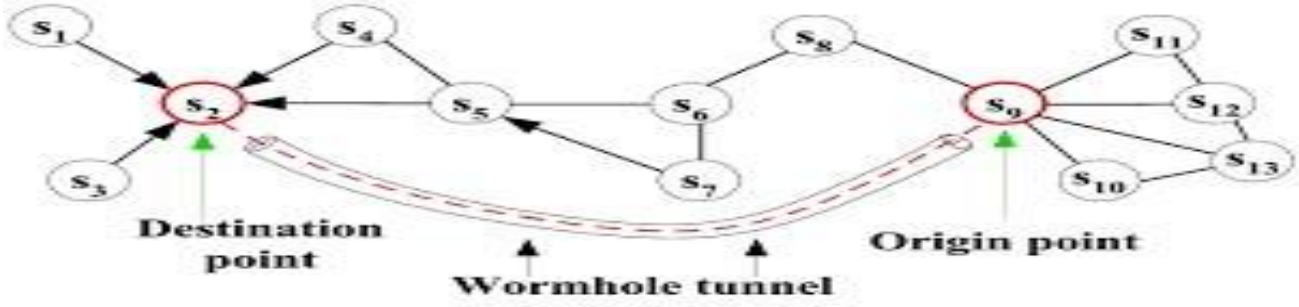

Fig.7. Attack via a Wormhole

5. Sybil Assault

A Sybil attack occurs when a computer is compromised and the hacker assumes several identities. In this assault, the attacker is able to simultaneously occupy many locations. A single node in the network having numerous identities significantly reduces the efficacy of fault tolerance.

Fig.8. Sybil Assault

6. Attack with a Sinkhole

In this assault, all communication from other nodes is diverted due to illegal access to a node inside the network. The routing method is used to carry out this action, along with luring the other nodes. Consequently, a number of attacks, including those that selectively forward packets, modify their content, or delete packets, might happen as a necessary part of the routing process.

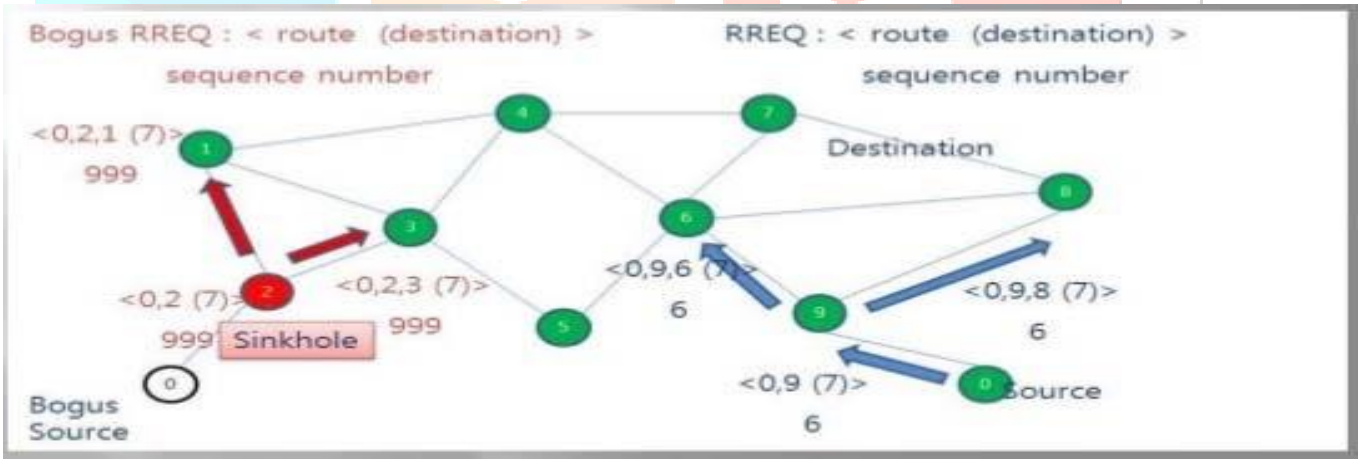

Fig.9. Attack with a Sinkhole

7. Denial-of-service attack

Authorized users can no longer access the services. The perpetrator bombards the victim's links with requests that seem authentic, leading to their deletion. As a result, the authorized users are denied access to all services.

8. Listening in

During this attack, the intruder eavesdrops on the information being transferred between the two nodes via the network. In this case, the information stays unchanged but its confidentiality is violated. The intruders might use this information to the detriment of the users.

B. Technology for identifying radio frequencies:

RFID technology is made up of several RFID tags and one or more RFID readers. The tags are affixed to things and have a designated address. The purpose of this tag is to give the thing in question a distinct identification. RFID tags are used for many different purposes, such as purchasing, tracking animals, monitoring food goods' temperature and humidity, tracking manufacturing, and access control. RFID technology is the target of several assaults. Here are some examples of the attacks:

1. Changes to Physical Data

The data is altered and the tags are physically obtained. Modification is achieved by the use of fault induction or memory writing. The intentional manipulation of data during the writing or processing phases is referred to as fault induction. Specialized tools like small charged needles or laser cutting microscopes may be used to write memories. As a consequence of these attacks, the tag data is erroneous. For example, an RFID tag attached to a manufactured object might provide false information about the product. In addition, the tag may be untraceable.

2. Cloning tags

The method entails copying the original tag identifier (id) onto a new tag that replaces the first one. Both the program and the tags are available for purchase. RFID tags do not need physical access protection, hence it is simple for an attacker to replace the original tag with a new one.

3. Switching tags

Tag swapping involves interchanging the tags of two distinct items. This kind of assault often takes place at retail establishments, when a high-value price tag is replaced with a lower-value one. The expensive goods is bought for a lower price.

4. Attacks that Deny Service

An RFID reader obtains the tag's unique ID when it makes an information request from a tag. It then compares that identification with the one stored in its database. In the event of a Denial of Service (DOS) attack, the tag is unable to provide the reader with its identity. There will be unstable communication between the tag and the reader, which will cause service outages.

CONCLUSION

The Internet of Things, or IoT, has emerged as a prominent and extensively used technical innovation. The information sent by sensors or RFID tags may include sensitive information that has to be secured against unwanted access. It is essential to ensure that the physical security of Internet of Things (IoT) devices is not compromised since there is no security between two nodes in the IoT. To safeguard vital infrastructure and real-time data, the Internet of Things (IoT) must include features like encryption, end-to-end environments, and access control. In the realm of cybercrime, staying one step ahead of the adversary is difficult. In the future, we anticipate more security measures for smart devices and more privacy laws for Internet of Things connections. This technology would make it simple for people to automate chores. Adoption of IoT including enhanced privacy protections, robust data security mechanisms, and ethical standards will undoubtedly win over customers' confidence and provide companies a significant competitive edge in the linked world.

REFERENCES

[1] Bahekmat, M., Yaghmaee, M. H., Yazdi, A. S., &Sadeghi, S. (2012). A Novel Algorithm for Detecting Sinkhole Attacks in WSNs. IJCTE, 4(3), 418-421.

[2] Balte, A., Kashid, A., &Patil, B. (2015). Security Issues in Internet of Things (IoT): A Survey.International Journal of Advanced Research in Computer Science and Software Engineering, 5(4), 450-455. ISSN: 2277 128X.

[3] Botta , A., de Donato, W., Persico, V. and Pescape, A., " Integration of Cloud computing and Internet of things: A Survey", Future Generation Computer Systems, Volume 56, March 2016, pp. 684700.

[4] Chowdhury, M., Kader, M. F., &Asaduzzaman. (2013). Security Issues in Wireless Sensor Networks: A Survey. International Journal of Future Generation Communication and Networking, 6(5), 97-116.

[5] D. Ruiz (Ed) et.al., Modelling the trustworthiness of the IOT, RERUM Deliverable D3.3, April 2016.

[6] Dlodlo, N., Foko, T., Mvelase, P., &Mathaba, S. (2012). The State of Affairs in Internet of Things Research Volume Issue,. The Electronic Journal Information Systems Evaluation, 15(3), (244- 258).

[7] Douceur, J. R. (2002). The Sybil Attack. Peer-to-Peer Systems, 251260.

[8] EU-China Joint White Paper on the Internet of Things, China Academy of Information and Communications Technology (CAICT) & European Commission –DG CONNECT, January 2016.

[9] Gianluca Aloi, Giuseppe Caliciuri , Giancarlo Fortino, Raffaele Gravina, Pasquale pace, Wilma Russo and Claudio Savaglio, A Mobile Multi Technology Gateway to enable IOT Interoperability, In proceeding of the IEEE IOTDI Conference, Berlin(Germany) 2016.

[10] Gubbi, J., Buyya, R., Marusic, S., &Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7), 1645-1660.

[11] Hossain, M. M., Fotouhi, M., &Hasan, R. (2015). Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things. 2015 IEEE World Congress on Services.

[12] Juels, A. (2006). RFID security and privacy: a research survey. IEEE J. Select. Areas Commun,24(2), 381-394.

[13] MacGillivray, Carrie, Worldwide Internet of Things Forecast Update, 2015-2019, International Data Corporation (IDC), February 2016.

[14] Mahalle, P. N., Anggorojati, B., Prasad, N. R., & Prasad, R. (2013). Identity Authentication and Capability Based Access Control (IACAC) for the Internet of Things. Journal of Cyber Security and Mobility, 1(4), 309-348.

[15] Maidamwar, P., &Chavhan, N. (2012). A Survey on Security Issues to Detect Wormhole Attack in Wireless Sensor
Network. IJANS, 2(4), 37-50.

[16] Mattern, F., &Floerkemeier, C. (2010). From the Internet of Computers to the Internet of Things. Lecture Notes in Computer Science, 242-259.

[17] Sarni, W., Mariani, J.; Kaji, J.; From Dirt to Data, The second green revolution and the Internet of Things. Deloitte Review, issue 18, 2016.

[18] Sathish Kumar, J., & R. Patel, D. (2014). A Survey on Internet of Things: Security and Privacy Issues. International Journal of Computer Applications, 90(11), 20-26.

[19] Singla, A., &Sachdeva, R. (2013). Review on Security Issues and Attacks in Wireless Sensor Networks. International Journal of Advanced Research in Computer Science and Software
Engineering, 3(4), 529-534.

[20] Sklavos, N., &Agarwal, V. (2008). RFID Security. From RFID to the Next-Generation Pervasive Networked Systems, 107-125.

[21] Soni, V., Modi, P., &Chaudhari, V. (2013). Detecting Sinkhole Attack in Wireless Sensor Network. International Journal of Application or Innovation in Engineering & Management
(IJAIEM), 2(2), 29-32.

[22] Sushma, Nandal, D., &Nandal, V. (2011). Security Threats in Wireless Sensor Networks.IJCSMS International Journal of Computer Science & Management Studies, 1(11).

[23] Tsai, C., Lai, C., &Vasilakos, A. V. (2014). Future Internet of Things: open issues and challenges. Wireless Netw, 20(8), 22012217.

[24] U.Farooq, M., Waseem, M., Khairi, A., &Mazhar, S. (2015). A Critical Analysis on the Security Concerns of Internet of Things (IoT). International Journal of Computer Applications, 111(7), 1-6.

[25] Vasilomanolakis, E., Daubert, J., Luthra, M., Gazis, V., Wiesmaier, A., &Kikiras, P. (2015). On the Security and Privacy of Internet of Things Architectures and Systems. 2015 International Workshop on Secure Internet of Things (SIoT).

[26] Z L., & T X. (2013). Threat Modeling and Countermeasures Study for the Internet of Things.JCIT, 8(5), 1163-1171.