International Journal of Multidisciplinary and Current Research ISSN: 2321-3124
Research Article Available at: http://ijmcr.com

An Elementary Research Scope and Constraints with IOT

Chandrakant D. Prajapati*, Dr. Krupa Bhavsar, Unnati P. Patel and Haresh P. Oza

Assistant Professor, Ganpat University, Kherva, Mehsana, Gujarat, India

Received 10 Aug 2020, Accepted 12 Oct 2020, Available online 15 Oct 2020, **Vol.8 (Sept/Oct 2020 issue)**

Abstract

The IoT is known as one of the most imperative zones of upcoming expertise in the Information Technology and is achieving huge devotion from a wide range of industries. The Internet of Things (IoT) opens opportunities for computing devices, home appliances, and software to share and communicate information on the Internet. The IoT consents objects to be sensed and/or controlled remotely across current network set-up, producing opportunities for more incorporation of the physical world into computer-based systems, and consequence in better accuracy, efficiency and economic advantage. In this paper, we begin with elementary information related to IoT with different challenges and four layered cyber security architecture. Protocols used in IoT systems can have security issues that can affect the entire systems. The Paper also comprises the Taxonomy of security attacks within IoT networks. We categorize different attacks into eight classifications which are erected to assist IoT users or developers for better awareness of the risk of security faults so that better defences shall be incorporated.

Keywords: *Internet of Things, IoT, IoMT, Smart Healthcare, layered architectures, Cyber security, Sensing Layer, attacks, SCA, PaaS, PaaS, Phishing Attack, Taxonomy, RFID.*

1. Introduction

The Internet of things (IoT) is a system of interconnected computing devices, mechanical and digital machines provided with unique identifiers (UIDs) and the ability to transfer the data over a network without requiring human-to-human or human-to-computer interface [2,3].

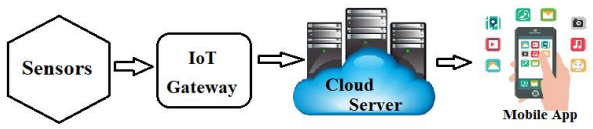

Fig. 1: IoT Basic Functionality

The Internet of things have evolved due to the convergence of multiple technologies, real-time analytics, machine learning, commodity sensors, and embedded systems traditional fields of embedded systems, wireless sensor networks, control systems, automation (including home automation), and others all contribute to enabling the IoT.

We can see in the Figure 1. It is illustrating the basic functionality for the IoT. Fundamentally IoT is a network in which all physical devices are connected to the internet through network devices.

*Corresponding author's ORCID ID: 0000-0003-1389-6363
DOI: https://doi.org/10.14741/ijmcr/v.8.5.8

IoT is use to control network infrastructure remotely, this technique has autonomous control feature with the use of this people can control devices without any human interaction.

The set of applications for IoT devices [4] are often divided into consumer, commercial, industrial, and infrastructure spaces. IoT devices are a part of the large concept of home automation, which can include lighting, heating and air conditioning, media and security systems.[5,6] A smart home or automated home could be based on a platform or hubs that control smart devices and appliances.[7,8] *The Internet of medical things (IoMT)* is an application of the IoT for medical and health related purposes, data collection and analysis for research, and monitoring.[9,10] The IoMT has been referenced as "Smart Healthcare" as the technology for creating a digitized healthcare system, connecting available medical resources and healthcare services.[11] Application of the IoT extends to all aspects of transportation systems (i.e. the vehicle, the infrastructure, and the driver or user[12]) for example like smart traffic control, smart parking, electronic toll collection systems, logistics and fleet management, vehicle control, safety, and road assistance.[13] IoT devices can be used to monitor and control the mechanical, electrical and electronic systems used in various types of buildings (e.g., public and private, industrial, institutions, or residential) in home automation and building automation systems.[14] The IoT

can be used in various manufacturing devices equipped with sensing, identification, processing, communication, actuation, and networking capabilities.[15] There are several IoT applications in farming[17] such as collecting data on temperature, rainfall, humidity, wind speed, pest infestation, and soil content. This data can be used to automate farming techniques, take informed decisions to improve quality and quantity, minimize risk and waste, and reduce effort required to manage crops.

2. Architecture of IOT

There are numerous technologies and sensors used to implement the idea of IoT. Here we can define four layered cyber security-oriented architecture for IOT.

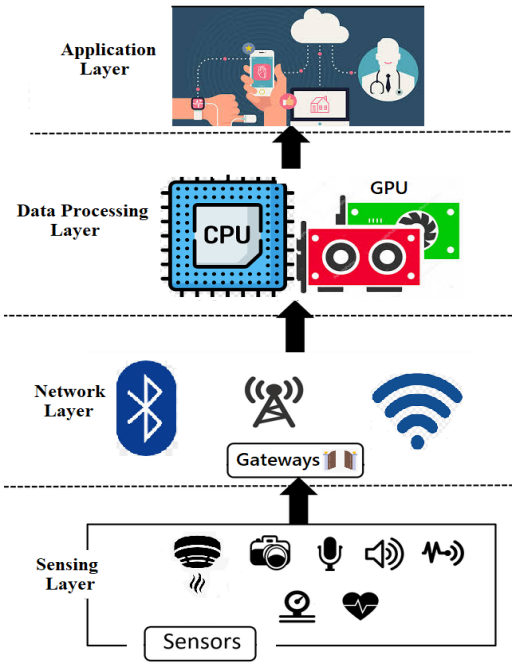

Fig. 2: Architecture of IOT Layer and Components

a) Sensing Layer

The sensing layer also known as perception layer, which has the responsibility to recognize things and gather the data from them. There are numerous types of sensors connected to the objects to gather information such as RFID, sensors and 2-D barcode. As per as requirement of applications, it can be selected. The sensors have the capacity to take measurements such as temperature, air quality, speed, humidity, pressure, flow, movement and electricity etc. A sensor can measure the physical property and convert it into signal that can be understood by an instrument. Sensors are grouped according to their unique purpose such as environmental sensors, body sensors, home appliance sensors and vehicle telematics sensors, etc. [34]. Cloud computing and social network perspective, there are some challenges exist in future Internet and also in current internet.

b) Network Layer

The network layer should be partitioned into two sublayers. One is a routing layer and the second is an encapsulation layer. Routing layer handles the packet transfer from source to destination. The encapsulation layer forms the packets [31]. Routing protocol: To operate on top of link layers PHY and MAC a distance vector and source routing, routing protocol has designed. It mainly focuses on the collection of periodic measurements in collection-based networks. The main feature of this protocol is to provide a routing solution for both lossy and low power networks [32]. It uses dynamically formed network topology to disseminate information over the network. This type of protocol generally suitable for where energy constrained devices are used in the applications. The mail advantages are: This protocol does not require translation gateways for accessing the nodes within the network from the outside world and provide end to end IP based solution, dynamic adaptation of control messages sending rating of the routing in the unstable network condition, it will consider the optimized network for different application scenarios and deployment. There are some limitations like: The protocol will not support the multipath routing; it will not consider the load and energy balancing [33].

c) Data Processing layer

This layer consists foremost data processing unit of IoT devices. The data processing layer takes data collected in the sensing layer and analyses the data to take decisions based on the result. In some IoT devices (e.g., smartwatch, smart home hub, etc.), the data processing layer also saves the result of the previous analysis to improve the user experience. This layer may share the result of data processing with other connected devices via the network layer [29]. There are some prominent challenges in data processing like Limited or no processing power, Communication restraints, Limited memory size, Real-time processing, handling high ingestion rate, preserving situation and context-awareness, Energy constraint, supporting scalability, providing fault tolerance, Ensuring security and privacy [30].

d) Application layer

The important functionality of the application layer is to determine service and take on service. This layer is a connection of IOT technologies and sector professional technologies. It can realize the wide smart application by providing numerous solutions. The application layer provides specific service to users through the analysed and processed perception data [26]. This layer mainly consisted of three parts, IOT client side, data storage module and data inquiry module [27]. The key issue for application layer is to share the information to the communities and secure the information safety.

3. Attack Taxonomy

Due to the heterogeneity of smart devices, communication protocols, applications, and services, the attacks appear to be malicious. We categorize different attacks into eight classifications. Details are in Figure 3.

Attacks Based on Devices are high-end and low-end device attacks. Attacks Based on Location are internal and external attacks. Attacks Based on Access Level are active and passive attacks [20]. Attacks Based on Information Damage include interruption, eavesdropping, modification, fabrication, replay, and man-in-the-middle attacks. Host-Based Attacks are users, hardware, and software attacks. Attacks Based on Strategy are physical and logical attacks. Protocol-Based Attacks are disruption and deviation attacks. Layer-Based Attacks are perception, network, middleware, and application attacks.

High-end device attacks involve high-power/full-fledged devices to launch attacks on the IoT system, while low-end device attacks involve low power devices to attack the IoT system.

Internal threats ("Insider") originate from inside the IoT network, and external threats ("Outsider") originate outside the IoT network [21]. In an internal attack, the attacker attempts to execute his own malicious code on smart devices in the IoT network. There are four types of internal attacks in practice: affected roles, unintentional roles, emotional attackers, and technically aware roles. An attacker tries to randomly, and without the user's knowledge, access IoT smart devices outside the network, remotely.

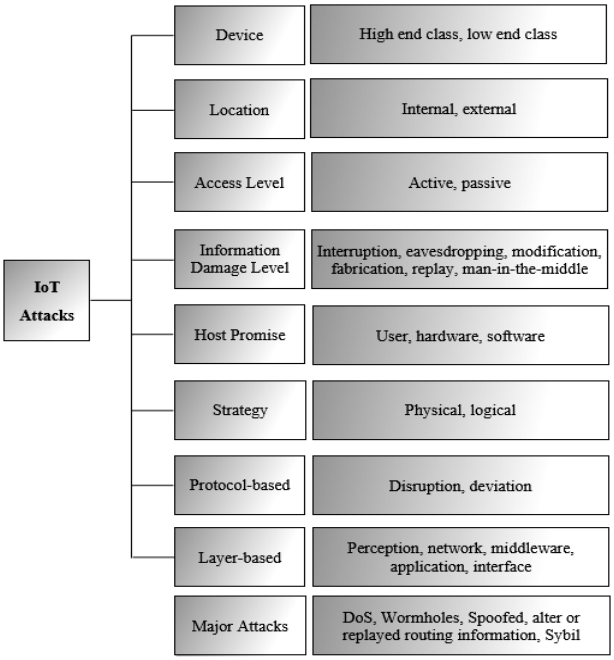

Fig. 3: Taxonomy of Cyber Security Attacks on IoT

Without disrupting information and communication in the IoT network, passive attacks involve monitoring and eavesdropping to recover information [22]. Contrary to passive attacks, active attacks directly affect the communication system in the IoT networks. Active attacks can circumvent or destroy smart devices and can destroy information or data [21].

The focus of the Interrupt Attack is on interrupting the availability of the system. If this occurs, resources will be exhausted and smart devices may shut down. Eavesdropping on the communication channel prevents the receiver device from selecting packets to send. RFID devices are vulnerable to eavesdropping attack. Attacks can alter or modify information or data in the IoT smart devices to mislead the communication protocol. This attack threatens the integrity of the IoT network security requirements. A Fabrication Attack occurs when an attacker inserts counterfeit data into the IoT architecture to create damage to the IoT information system and to threaten IoT authentication [23]. Credential information or data (such as passwords or keys) associated with actual users may be misappropriated and abused. Attackers attack software because of IoT device exhaustion or resource buffer overflow vulnerability [24]. Attackers injecting malicious code or stealing the actual driver or connecting to the device is a Hardware Attack. Since most smart devices are run in an outdoor environment, physical attacks are likely to tamper with hardware. Physical attacks are similar to hardware attacks. Logical Attacks bring dysfunction to communication systems over the IoT network without harming physical devices. Attackers can attack IoT in an abnormal manner. External attackers may pretend to be insiders and may execute malicious code on the IoT network. Thus, attackers can attack protocols by disrupting internal or external networks: key management protocol, data aggregation protocol, synchronization protocol, etc. Deviation Attacks have two target protocols: application protocol and the network protocol [25].

4. Characteristics

IOT should have the following three characteristics

1. *Broad Perception*: Using RFID, sensors, and two-dimensional barcode to obtain the object information at anytime and anywhere, it will be a new opportunity. Using it, information and communication systems can be invisibly embedded in the environment around us. Sensor network will enable people to interact with the real world remotely. Identification technologies mentioned here include objects and location identifications. Identification and recognition of the physical world is the foundation of implementing overall perception.

2. *Reliable Communication*: Through a variety of available radio networks, telecommunication networks, and Internet, objects information can be available in any time. Communication technology

here includes a variety of wired and wireless transmission technologies, switching technologies, networking technologies, and gateway technologies. IoT further creates the interaction among the physical world, the virtual world, the digital world, and the society. Machine to machine (M2M), furthermore, is the key implementation technology of the Network of Things, which represents the connections and communications between M2M and Human to Machine including Mobile to Machine.

3. *Intelligent Processing:* By collecting IoT data into databases, various intellectual computing technologies including cloud computing will be able to support IoT data applications. The network service providers can process tens of millions or even billion pieces of messages instantly through cloud computing. Cloud computing technology will thus be the promoter of IoT.

Conclusion

It is concluded that this paper giving an insides about introduction of internet of thing, different application of IOT like medical, manufacturing, industrial, transportation, education, governance, mining, habitat etc., given a picture of all proposed layered architecture of IOT, also highlighting the security attacks that can occur on each layer and affect the IOT applications.

References

[1]. S. Haller, S. Karnouskos, and C. Schroth, "The Internet of Things in an Enterprise Context," in *Future Internet – FIS 2008 Lecture Note in Computer Science* Vol. 5468, 2009, pp 14-28

[2]. *Rouse, Margaret (2019). "internet of things (IoT)". IOT Agenda. Retrieved 14 August 2019.*

[3]. Brown, Eric (20 September 2016). "21 Open Source Projects for IoT". *Linux.com*. Retrieved 23 October 2016.

[4]. Vongsingthong, S.; Smanchat, S. (2014). "Internet of Things: A review of applications & technologies" (PDF). *Suranaree Journal of Science and Technology*.

[5]. "The Enterprise Internet of Things Market". *Business Insider*. 25 February 2015. Retrieved 26 June 2015.

[6]. Perera, C.; Liu, C. H.; Jayawardena, S. (December 2015). "The Emerging Internet of Things Marketplace From an Industrial Perspective: A Survey". *IEEE Transactions on Emerging Topics in Computing*. 3 (4): 585–598.

[7]. Kang, Won Min; Moon, Seo Yeon; Park, Jong Hyuk (5 March 2017). "An enhanced security framework for home appliances in smart home". *Human-centric Computing and Information Sciences*.

[8]. *"How IoT & smart home automation will change the way we live". Business Insider. Retrieved 10 November 2017.*

[9]. Kricka, LJ (2019). "History of disruptions in laboratory medicine: what have we learned from predictions?". *Clinical Chemistry and Laboratory Medicine*.

[10]. Gatouillat, Arthur; Badr, Youakim; Massot, Bertrand; Sejdic, Ervin (2018). "Internet of Medical Things: A Review of Recent Contributions Dealing with Cyber-Physical Systems in Medicine"

[11]. Dey, Nilanjan; Hassanien, Aboul Ella; Bhatt, Chintan; Ashour, Amira S.; Satapathy, Suresh Chandra (2018). *Internet of things and big data analytics toward next-generation intelligence*

[12]. Mahmud, Khizir; Town, Graham E.; Morsalin, Sayidul; Hossain, M.J. (February 2018). "Integration of electric vehicles and management in the internet of energy". *Renewable and Sustainable Energy Reviews*.

[13]. "Key Applications of the Smart IoT to Transform Transportation". 20 September 2016

[14]. Ersue, M.; Romascanu, D.; Schoenwaelder, J.; Sehgal, A. (4 July 2014). "Management of Networks with Constrained Devices: Use Cases". *IETF Internet Draft*.

[15]. Yang, Chen; Shen, Weiming; Wang, Xianbin (January 2018). "The Internet of Things in Manufacturing: Key Issues and Potential Applications"

[16]. Meola, A. (20 December 2016). "Why IoT, big data & smart farming are the future of agriculture". *Business Insider*. Insider, Inc. Retrieved 26 July 2018.

[17]. 2327-4662 (c) 2018 IEEE. See http://www.ieee.org/ publications_standards/publications/rights/index.html for more information.

[18]. DOI 10.1109/JIOT.2018.2869847, IEEE Internet of Things Journal > replace this line with your paper identification number 4

[19]. Jayavardhana, G., Rajkumar, B., Marusic, S. and Palaniswami, M. (2013) Internet of Things: A Vision, Architectural Elements, and Future Directions. Future Generation.

[20]. R. H. Weber, "Internet of things-new security and privacy challenges,"Comput. Law Security Rev., vol. 26, no. 1, pp. 23–30, 2010 13

[21]. M. Hossain, R. Hasan, and A. Skjellum, "Securing the Internet of Things:A Meta-Study of Challenges, Approaches, and Open Problems," Distributed Computing Systems Workshops (ICDCSW), 2017 IEEE 37th International Conference on. IEEE, 2017, pp. 220-225 38

[22]. A. Mayzaud, R. Badonnel, and I. Chrisment, "A taxonomy of attacks in rpl-based internet of things," International Journal of Network Security, vol. 18, no. 3, pp. 459–473, 2016. 40

[23]. S. Alam and D. De, "Analysis of security threats in wireless sensor network," International Journal of Wireless and Mobile Networks,

[24]. G. P. Hancke and S. C. Centre, "Eavesdropping Attacks on High-Frequency RFID Tokens," In Proc. Workshop Radio Frequency Identification Security, Jul. 2008, pp. 100–113.

[25]. M. Hossain, M. Fotouhi, and R. Hasan, "Towards an analysis of security issues, challenges, and open problems in the IoT," In Services (SERVICES), 2015 IEEE World Congress on IEEE, 2015, pp. 21-28.

[26]. Zhihong Yang, Yingzhao Yue, Yu Yang, Yufeng Peng, Xiaobo Wang, & Wenji Liu. (2011). *Study and application on the architecture and key technologies for IOT. 2011 International Conference on Multimedia Technology.* doi:10.1109/ icmt.2011.6002149

[27]. Handong Zhang, & Lin Zhu. (2011). *Internet of Things: Key technology, architecture and challenging problems.* 2011 IEEE International Conference on Computer Science and *Automation Engineering.* doi:10.1109/csae.2011.5952899

[28]. Wang, F., Hu, L., Zhou, J., & Zhao, K. (2015). *A Data Processing Middleware Based on SOA for the Internet of Things. Journal of Sensors, 2015, 1–8.* doi:10.1155/2015/827045

[29]. Amit Kumar Sikder, Giuseppe Petracca, Hidayet Aksu, Trent Jaeger, and A. Selcuk Uluagac, *"A Survey on Sensor-based Threats to Internet-of-Things (IoT) Devices and Applications",* February 2018.

[30]. Pijush Kanti Dutta Pramanik and Prasenjit Choudhury, *"IoT Data Processing: The Different Archetypes and Their Security and Privacy Assessment"* September 2019.

[31]. Cheena Sharma; Dr. Naveen Kumar Gondhi,‖ Communication Protocol Stack for Constrained IoT Systems‖, 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU)‖, pp. 1 – 6, 2018.

[32]. S. Umamaheswari ; Atul Negi, —*Internet of Things and RPL routing protocol: A study and evaluation‖, International Conference on Computer Communication and Informatics* (ICCCI)‖, pp. 1 – 7, 2017.

[33]. Srinivasa A H, Dr.Siddaraju, "*A Comprehensive Study Of Architecture, Protocols And Enabling Applications In Internet Of Things (Iot)*", International Journal Of Scientific & Technology Research Volume 8, issue 11, november 2019.

[34]. Keyur K Patel, Sunil M Patel, *"Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges",* International Journal of Engineering Science and Computing, May 2016.