International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 4 Issue: 12
ISSN: 2454-4248
132 – 135

End-to-End IoT Architecture Vulnerabilities and Attacks

Rajendra Kumar
Department of Computer Science, Faculty of Natural Science,
Jamia Millia Islamia, New Delhi-110025 (INDIA)
Email : rkumar1@jmi.ac.in

Abstract-The communication between physical object was a dream of researchers but with the introduction and advancement in internet it becomes an easy task. The technology is called *internet of things (*IoT). This paper aims at providing more detailed study on internet of things and how real world physical objects communicate. The role of sensors, embedded technologies in the objects, physical topologies, networks among the devices that is the end to end view of the IoT architecture. With the advantages black side of internet also come into picture that makes its crucial to analyse the network and finding the vulnerabilities associated The main cause of concern is the security and privacy that are been shown and talked about in the paper. In the proceeding sections we have discussed the end to end view architecture of IoT, vulnerabilities and attacks possible in IoT environment. Later, a small study of edge computing is also shown.

Keyword: *Edge computing, Internet of things, security, vulnerability, attacks.*

*****

I. INTRODUCTION

According to a survey, it is estimated that by 2020, market volume of machine to machine communication will reach 223.4 billion US dollars, making IoT a big and powerful industry from economic growth perspective[1, 2, 3].So, it is very important to study this technology in detail and find the vulnerabilities and attacks possible in securing running this powerful industry. The term Internet of Things was founded in the year 1999 to promote RFID (radio frequency identification) technology. When the devices can represent themselves digitally it becomes easy to control them from anywhere and everywhere. The connectivity between these objects helps to collect more valuable and voluminous dataand ensure more ways of improving safety and IoT data security. IoT has its role in various fields especially in business as it can be a transformational force that brings a revolution in companies through IoT analytics and hence deliver better results. With thesensors, actuators, connectivity tracking of devices becomes possible, this new emerging field can benefit from real-time analytics and insights. In a new report,by Forbes on major predictions on IoT says IoT Moves from Experimentation scaleto Business Scale[2, 3].A recent research by Forrester predicts that the IoT will become the backbone of future customer value, the future is IoT, IoT platforms.This heterogeneous technology comes with major security and privacy concerns. Many researchers are working in this area and established solutions for security and privacy through many modern techniques like cryptography, block chain, artificial intelligence, machine learning. The Internet of things is not like it was just a few years ago.it is growing rapidly and devices that earlier had only few functions have now become advanced and easy to handle because of this advance technology. security will remain a key concern.

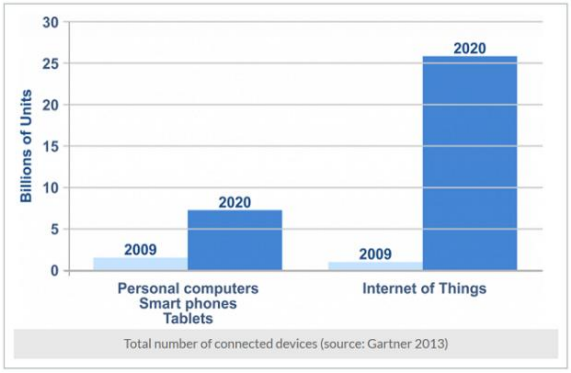


Fig1: ConnectedDevices

II. LITERATURE REVIEW

In this section of the paper, a brief literature review of existing work in the area of IoT using machine learning classifiers is provided particularly in the area of health care and monitoring, hence providing the application of artificial intelligence in the area of IoT.

Today, sensing and communication with embedded software in the devices has become versatile for healthcare systems[4, 14]. The smartness of these devices is based on decision taking capabilities using cloud computing, sensing technology, communication technology, location technology. In [5, 6, 7, 8] author presented an intelligent IoT based human activity recognition system using data mining techniques. The author proposed a user-dependent data mining approach for off line human activity classification by utilizing the dataset containing 12 physical activities for human activity recognition.at the end Random forest and SVM showed maximum accuracy of 99.89% and concluded that these can be used for human activity recognition.Large number of sensors deploy on human body can bring dizziness in subject's body hence leads to incorrect sensor measurement. The placement of sensors on correct location for correct data collection is also a challenging task.

 ISSN: 2454-4248
132 – 135

Therefore, maintaining high and correct classification of activity with minimum sensors is a matter of concern. Author[9] has classified the daily human activities, humans equipped with wearable inertial sensors(one on right thigh, chest, left ankle),12 daily life living activities(lying down, lying, walking, stair ascent and standing up,standing, stair descent, sitting, sitting down, sitting on the ground, from lying to sitting on the ground,from sitting to sitting on the ground) with emphasis on elderly subjects' activities. Then the performance comparison of supervised(k-Nearest Neighbour (k-NN), Support Vector Machines (SVM), Supervised Learning Gaussian Mixture Models (SLGMM) and Random Forest (RF)) and non-supervised(k-Means, Gaussian Mixture Models (GMM) and Hidden Markov Model (HMM)) algorithm is performed and showed KNN best among supervised and HMM among unsupervised.

III. IOT APPLICATIONS

One of the prominent application of IoT is for smart cities.According to Gartner,by 2050, around 70 percent of the world's population will shift to cities [3]. This is placing a strain on the existing infrastructure globally. To accommodate this new demand, municipalities turning to the Internet of Things innovation to enhance the services provided, improve interaction and communication, reduced cost of operation. The applications of IoT are diverse and numerous making the technology widely acceptable, some of them are discussed in fig 2.each area is so wide that researchers are working on challenges that are prevailing.

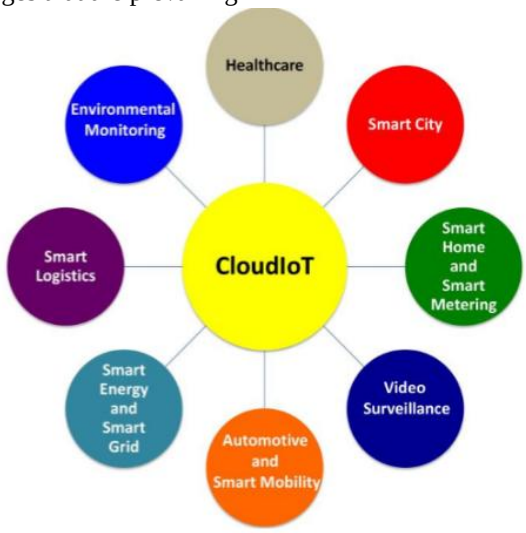


Fig2: AapplicationDomains

IoT will be the source of valuable data on Earth. It is not beyond imagination to say what if a medical history of human, allergies to medication are to be digitized as a part of an initiative in electronic health field. Healthcare associated people will be able to understand and leverage the multiplicity of big data from connected sub systems to make informed patient care decisions as well as prophecy current and future health trends. IoT potential can be seen to support healthcare by connecting people, applications, data on one hand and sensors, devices that collect contextual and biometric data.

IoT technology based systems canaddress a broad set of health problem ranging from well-being to sickness, physical to mental health,temporary disabilities to chronic disease preventive care to treatment or rehabilitation. In this situation,watches, smartphones and other smart devices as well as additional sensors, devices, and equipment can be connected to the IoT networks and provide information about the sick person, and the sick person environment,the sick person actions.

IV. IOT ARCHITECTURE

A. End to End view of IoT Architecture

The IoT functionality is depicted in figure 3 that is classified as follows:

1) *Sensing*: the end nodes/sensors are the devices that are responsible for sensing desired applications like trash container sensors for waste management through leveling of wastage in container. This can be called as the data sensing and storing node.

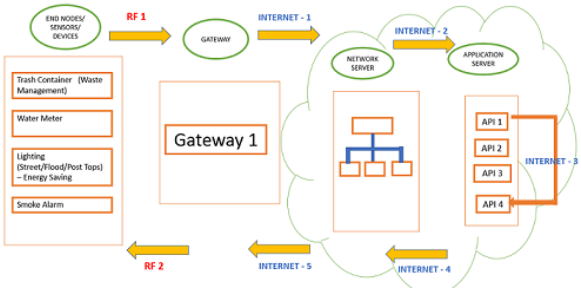


Fig 3: End to End IoT Architecture

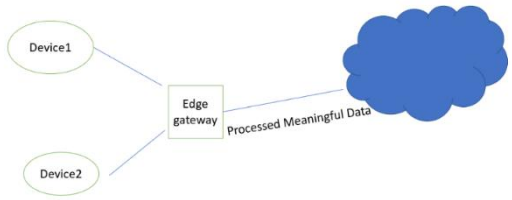
2) *Pairing*:pairing between nodes/ sensors + nodes/ sensors + gateway by using local networks like RF/GPRS/GSM etc. The pairing can be serve as the sensor access point by the hackers and attackers.

3)*Communication*:TheIoT communication involves exchange and sharing of information among the devices. with this lots of communication and exchanges the infrastructure of iot is in consistent from security perspective and vulnerable to information and data losses. The medium of communication between the devices is the decision point for the attackers. The gateway communicates to cloud through internet 1(GSM/3G etc) as shown in the figure above.

4)*CloudComputing*.now API in cloud will analyze the communication and desired action will be computed through specific API. All the data from all the way reaches to application server for any kind of monitoring and control. Bigger Database and server is required to handle large amount of data. There is a need of all time internet connectivity to reduce any type of losses.

This is the place which gave way to edge computing which has tremendous applications in city and campus automation by allowing your cloud to reach near the data produced by devices. Now, the data need not to travel all the way to the cloud. Only the important data need to travel across the network. This helps in data processing and storage at edge for backup and internet independent control.

 ISSN: 2454-4248
132 – 135



b). Network protocol and IoT

In Internet of Things connected devices embedded with sensors actuators exchange information or data over the internet. The common protocols used for the internet TCP, UDP, HTTP. The protocols created specifically for internet of things like MQTT,CoAP. When designing IOT device it is very important to know how local network will connect to the internet. This is performed by using a gateway or can built this capability directly to the IoT device.TCP/IP- the internet protocol suite is the heart of internet. The protocol suit consists of seven layer also popular as OSI reference model.

TABLE I. LAYER WISE PROTOCOL DESCRIPTION

Application layer	Where the embedded applications live Telnet, FTP, TFTP, HTTP, BOOTP, DHCP, SNMP, Socket API
Presentation layer	
Session layer	
Transport layer	TCP,UDP
Network layer	Where the internet lives, can find the ubiqtous IP address IP,ARP,ICMP
Data link layer	Raw bits and bytes are transmitted in the form of frames, wired and wireless method of sending data. PPP,SLIP,ETHERNET
Physical layer	Responsible for sensing using RFID,BLE etc

V. VULNERABILITIES AND ATTACKS IN IOT

It is being predicted that by 2025 approximately 75 million connected IoT devices will be there[1], most of the firmware running on these devices have majorsecurity concerns and are susceptible to cyber attacks. Inoct2016, aDDOS(Distributed Denial of service) attack was launched on service provider Dyn which lead internet to go down including twitter, Netflix. this attack was made possible by a malware called Mirai.A malware VPN Filter granted control to infected devices through affecting routers and allow the option of turning off and taking them out of the network range(offline)[6, 10].The smart cities cannot be made in a single day[2, 11].We started exploiting the vulnerabilities in smart cities. Maximum vulnerabilities were caused due to security flaws like using default passwords and leaving networks without authentication which made easy access of the system to hackers. Smart car by tesla a vulnerability to a key fob attack was discovered which is a technique that is used to steal the cars [2, 12]. The reason was an easily crackable,40-bit cipher and lack of authentication. [1, 13, 17] the vulnerabilities in healthcare devices were detected , due to poor authentication and encryption the device software that is used to control the pacemakers settings was infected by malware by accessing its transmitter.The webcam hack is also one of the most important security concern which can be compromised by obtaining a camera's IP address [14].

Attacks possible in IoT

The security and privacy in IoT is a popular and big challenge in today's technology world[15, 16, 18, 19].

There are many views regarding the security concern. In this study, Firstly the communication architecture is shown. This shows how the communication between things (IOT) occur in a controlled environment. We are constantly generating huge amount of data, backup by cloud which is a data center or a data server and we use array of devices to access these data. due to so many access points, tons of data, cyber-attack comes into existence. The attackers are so intelligent that the malware they produce bypass the firewalls. In this era of digitization, every communication is digital this makes space for more strong cyber security. In this study, we have shown the different types of attacks that are possible when the devices are connected to local network or internet. secondly, a case study of security breach in smart city solution is also shown.

Types of cyber-attacks that are possible in a communication network:

1. Malware: it represents diversity of cyber threats like Trojans, worms, virus. Malware is a code with malicious intent of particularly stealing data and now the devices can be controlled without the knowledge of a user.in botnet scenario it is very common practice.
2. Phishing: these are the attacks sent by email and asks users to add certain details and behave so legitimate that it becomes difficult to differentiate which is legitimate email.
3. Password attacks:cracking of password to get access to system getting unauthorized access to user system.
4. DDOS(distributed denial of service): most dangerous attack that focuses on stopping the services of an attacked network, during attack propagation attackers send huge volume of data and traffic through the network to make many connection requests as a result, network becomes overloaded and start denning requests hence known as denial of services. A very popular Mirai attack 2016 that is a malware strain causes DDOS [6].
5. Sinkhole attacks:in these type of network attacks,the malicious node announces a beneficial route that is false and attract all nodes to redirect their packets.

 ISSN: 2454-4248
132 – 135

6. Black hole attacks:in these,the malicious device announces shortest false path to the destination and starts dropping the packets thus creating a black hole.
7. Man in the middle attack:impersonation the end point in a network communication that is the connection from smartphone to website the man in middle can obtain the info from end user and entity of communication.

VI. CONCLUSION

In this study, a simple IoT perspective by including end to end architecture, network protocols, vulnerability and attacks is presented. The security remains a key concern in IoT environment. The communication between devices and storage of data on cloud is the heart of IoT architecture that is to be made secure for proper functioning. There are different threats and attacks discussed in this study which can harness the proper functioning of devices. we have to introduce some measures that can provide security and make uninterrupted services possible in IoT. The whole process starts with devices that are smart like watches, smartphones, bulbetc, which communicate with IoTplatform. In the end, this paper will give a better understanding for the new researchers in this field of IoT application domains

REFERENCES

[1] IoT Security:"An End-to-End View and CaseStudy" Zhen Ling, Kaizheng Liu, Yiling Xu, Chao Gao, YierJin, Cliff Zou, Xinwen Fu, and Wei Zhao.

[2] L. Atzori, A. Iera, and G. Morabito, "Theinternet of things: A survey," Computer Networks, vol. 54, no. 15, pp. 2787–2805,Oct. 2010.

[3] L. Columbus, "Roundup of internet of things forecasts and market estimates," https://www.forbes.com/sites/louisColumbus/2016/1 1/ 27/ roundup -of -internet -of-things- forecasts-and-market-estimates2016/#27232e3 d292d, 2016.

[4] Z. Ling, K. Liu, Y. Xu, Y. Jin, and X.Fu, "An end-to-end view of iot security and privacy," in Proceedings of the 60th IEEE Global Communications Conference (Globecom), 2017

[5] O. Arias, J. Wurm, K. Hoang, and Y. Jin,"Privacy and security in internet of things and wearable devices," IEEE Transactions on MultiScale Computing Systems, vol. 1, no. 2, pp. 99–109, 2015

[6] https://www.pentasecurity.com/ blog/ 4- shocking-iot-security-breaches-2018/

[7] Poongodi, M. & Bose, S. Arab J SciEng https://doi.org/10.1007/s13369-015- 1822-7, 2015

[8] IoT based Mobile Healthcare System for Human Activity Recognition byAbdulhamitSubasi,MariamRadhwan, RabeaKurdi,KholoudKhateeb

[9] Ferhat Attal, Samer Mohammed, MariamDedabrishvili ,FaicelChamroukhi , LatifaOukhellou and YacineAmirat Physical Human Activity Recognition Using Wearable Sensors

[10] Oleksiy Mazhelis, PasiTyrväinen,"Aframework for evaluating Internet-of-Things platforms: Application provider viewpoint", IEEE World Forum on Internet of Things (WF-IoT), IEEE, Seoul, South Korea, March 2014

[11] J. Wurm, K. Hoang, O. Arias, A.R.Sadeghi, Y. Jin, "Security analysis on consumer and industrial IoT devices", Proc. 21st Asia and South Pacific Design Automation Conference (ASP-DAC), pp. 519-524, Jan. 2016.

[12] Jianli Pan, Raj Jain Subharthi Paul, Tam Vu,AbusayeedSaifullah, Mo Sha," An Internet of Things Framework for Smart Energy in Buildings: Designs, Prototype and Experiments",IEEE Internet of Things Journal, 2 (6) (2015), pp. 527-53

[13] Ahmad A., Xiaoyun Z., Daji Q., AhmedK.," An Energy-Efficient Relaying Scheme for Internet of Things Communications", IEEE International Conference on Communications (ICC), Kansas City, MO, USA, May 2018

[14] M. Busch, C. Hochleitner, M. Lorenz, T.Schulz, M. Tscheligi, and E. Wittstock, "All in: targeting trustworthiness for special needs user groups in the Internet of Things," in Lecture Notes in Computer Science, M. Huth, N. Asokan, S. Čapkun, I. Flechais, and L. Coles-Kemp, Eds. Berlin: Springer, pp. 223–231, 2013.

[15] Peter Corcoran, Claudia Costache, "Biometrictechnology and smartphones: A consideration of the practicalities of a broad adoption of biometrics and the likely impacts", Technology and Society (ISTAS) 2015 IEEE International Symposium on, pp. 1-7, 2015.

[16] Benjamin Yee Shing Li ; Lam Fat Yeung ; KimFung Tsang," Analysing traffic condition based on IoT technique", IEEE International Conference on Consumer Electronics - China, IEEE, Shenzhen, China, April 2014

[17] Joao Lima, "Behold the 10 biggest IoTinvestments," Computer Business Review, April 9, 2015

[18] I. Ganchev, Z. Ji, M. O'Droma, "AGenericIoT Architecture for Smart Cities", 25th IET Irish Signals & Systems Conf. 2014 and 2014 China-Ireland Int'l. Conf. Info. and Commun. Technologies, pp. 196-99, 2013.

[19] KabalciErsan, AlperGorgun, YasinKabalci,"Design and implementation of a renewable energy monitoring system", Power Engineering Energy and Electrical Drives (POWERENG) 2013 Fourth International Conference, 2013.