iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** I **Month of publication:** January 2018

DOI: http://doi.org/10.22214/ijraset.2018.1057

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor :6.887
Volume 6 Issue I, January 2018- Available at www.ijraset.com

Summarization of IOT Protocols, applications, protocols, Security Concerns

Hyma Birudaraju[1], M. Kireet[2]
[1]*Assistant Professor, Gurunanak Institutions Technical Campus, Hyderabad*
[2]*Lecturer, JNTU College of Engineering, Hyderabad*

Abstract: ***The immense growth of hand-held devices extended the usage of the IOT devices among different users. The majority of data transfer today is done through by the usage of IOT devices. IOT-the Internet of things is system of physical devices, home appliances and other different devices connected to exchange data. In this paper we have summarized about the IOT-its importance, protocols which are used in IOT, different types of applications of IOT, risks that are involved when the data exchange is done through IOT. The major contribution of this paper it to analyse the security risks, summarize the existing protocols used in IOT devices and study the real-time risks, attacks in IOT devices.***
Keywords*:* ***IoT(Internet of things), security risks in IoT, IoT protocols***

I. INTRODUCTION

Today the Internet has clad to be universal, has touched much each facet of the world, and is influencing human life in incomprehensible ways that we have a tendency to square measure presently coming into a time of considerably additional inevitable convenience wherever a good assortment of machines are related to the online. we've got been into the era of IOT. This term has been characterized by various creators in a wide range of ways. Vermesan et al. [1] characterize the IOT as basically cooperation between the physical and computerized universes. The computerized world connects with the real-time world utilizing a plenty of devices like sensors and actuators. Another definition by Pea-Lpez et al. [2] characterizes the Internet of Things as a worldview in which processing and systems administration abilities are implanted in any sort of possible question. We utilize these abilities to inquire the condition and to change its state if conceivable. In like manner speech, the IOT alludes to another sort of world where every one of the gadgets or products or devices (all this paper we used the word gadgets in place of devices or products) that we utilize are associated with a system. We can utilize them cooperatively to accomplish complex assignments that require a high level of insight.

For this knowledge and interconnection, IoT gadgets are furnished with inserted sensors, actuators, processors, and handsets. IoT isn't a solitary innovation; rather it is an agglomeration of different advances that cooperate pair.

Sensors and actuators are gadgets, which help in cooperating with the physical condition. The information gathered by the sensors must be stored and prepared wisely so as to get helpful surmising (suppose that something is true without having evidence to confirm it) from it. An actuator is a gadget that is utilized to impact an adjustment in the earth, for example, the temperature controller of a ventilation system. Sensors, actuators, process servers, and the correspondence arrange shape the centre foundation of an IoT structure. In any case, there are numerous product viewpoints that should be considered. Initially, we require a middleware that can be utilized to associate and deal with these heterogeneous parts. We require a considerable measure of institutionalization to interface a wide range of gadgets. The Internet of Things finds different applications in medicinal services, wellness, instruction, diversion, social life, vitality protection, condition checking, home computerization, and transport frameworks. As the no of IOT devices increased their arises the security concerns related to the devices. IoT security is mainly concerned about defending or ensuring the associated products and systems in the Internet of things (IoT). Many Industrial—Security-Experts consider the IOT security as the first step for the success of many IOT devices, as the sensitive data is handled by many devices ensuring security is concerned as the primary concerns for the devices

II. ARCHITECTURE OF IOT

The essential architecturee is a three-layer design [5] as appeared in Figure 1 . It was presented in the beginning periods of research here. It has three layers, the-Perception- layer,the- network- layer, and the-application- layers.

A. The-perception

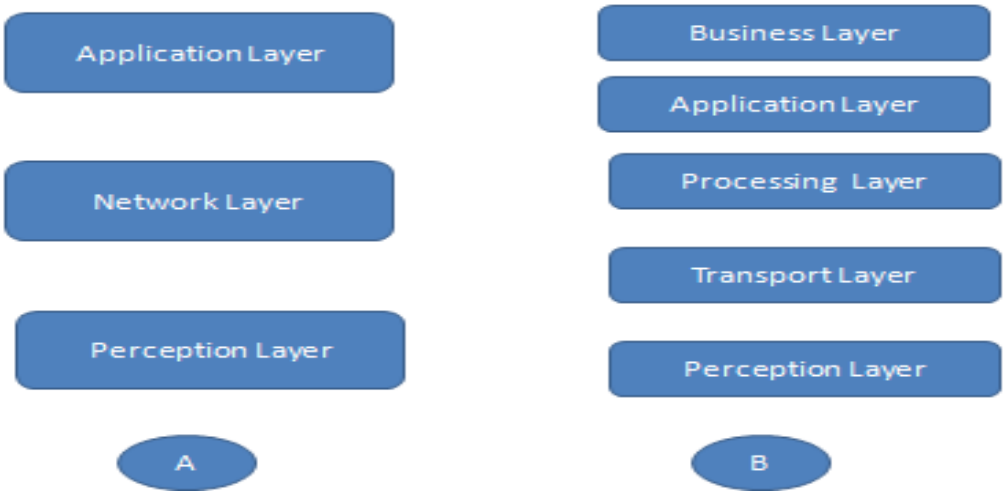
layer is the physical layer, contains sensors for detecting and assembling data about nature. It detects some physical parameters or recognizes other shrewd protests in the earth.

B. The-Network

layer is in charge of interfacing with other smart things, arrange gadgets, and servers. Its highlights are additionally utilized for transmitting and preparing sensor information.

C. The-Application

layer is in charge of conveying application particular administrations to the client. It characterizes different applications in which the Internet of Things can be sent, for instance, brilliant homes, savvy urban areas, and keen wellbeing. The three-layer design characterizes the fundamental thought of the Internet of Things, yet it isn't adequate for examine on IoT in light of the fact that examination regularly concentrates on better parts of the Internet of Things. That is the reason, why the numerous more layered structures proposed in the writing. One of them is 5-layer engineering, which furthermore incorporates the processing and business layers [5][6]. The 5-layers are the-Perception, the-transport, processing, the-application, and the-business layers. The part of the-perception and the-application layers is similar to the engineering with three layers. The-transport layer exchanges the Sensor information from-the discernment layer to the processing-layer and the other way around through systems, for example, remote, 3G, LAN, Bluetooth, RFID, and NFC The-processing layer is otherwise called mid-dleware layer. It stores, examines, and forms enormous measures of information which originates from the-transport layer, which can oversee and give a various arrangement of administrations towards the lower layers. It utilizes numerous advances, for example, databases, distributed computing, and huge information processing modules.



The-business layers deals with the entire IoT frame-work, including the applications, the-business and the-benefit models, and clients' security. Another engineering proposed by Ning and Wang [7] is enlivened by the layers-of- processing in the human mind. It is motivated by the insight and capacity of people to think, feel, recollect, decide, and respond to the physical condition. Information processing hubs and savvy passages. Third-one is the system of nerves, which relates to the systems administration segments and sensors.

III. IOT SECURITY AND IT'S NEED

IoT security is the area of endeavour deals with providing protection to the devices which are connected and the networks in the Internet of things. IOT-security is significantly concerned about defending or ensuring the associated products and systems connected. The major concern is security has not generally been considered at product configuration level. The vast majority of the IoT products are frequently solded with default and un-patched installed working frameworks and programming. In the wake of acquiring, buyers frequently neglect to change the essential default passwords on IOT gadgets and some of them neglect to choose the strong unbreakable passwords. To enhance security, an IoT product that should be open over online, should be segregated into its own-network and access of network should be based on the strong privileges policy. The network-system section will be then supervised to identify the potential anomalous traffic- analysis, based on that the action should be taken. Major issues**:** Most of the IOT devices are deployed in the environment where charging is not available as a result battery extension is still one of the major issue in IOT. One more issue is Cryptographic algorithms like conventional cryptography cannot work on IOT systems as the devices has limited storage cannot handle or satisfy the requirements of advance cryptographic algorithms for computing.

A. Major Security Concerns in IoT

1) Networks: The Unauthorized-access-to data and service, dos Modification of information, viruses and different type of malware attacks, buffer overflows etc.

2) Front end sensors and equipment : Unauthorized access to data and service ,denial of service attacks, attacks and privacy analysis on machine 2machine information Back end of IT systems : Safety Management of code resources ,replacement of operators

III. IOT PROTOCOLS

IoT semantically implies an "overall system of interconnected items or objects remarkably known based on the standard protocols." This implies a colossal no. of items perhaps heterogeneous objects are associated with the procedure. In IoT, unique Identification of items or objects and their representation and also the exchange of information which is the most challenging issue.

A. Existing Protocols

IEEE 802.15.4 which are called Low-energy communications at the physical (PHY) and Medium Access Control (MAC) layers. 802.15.4 mainly concentrates to set the rules for the communications possible at the lower layers of the stack and lays down the base for IoT communication protocols at higher layers. Low-energy communicatetion eenvironments which are are using 802.15.4 spare at most 102 bytes for the transmitting the data which is at higher layers of the stack, a value which can be considered as lesser than the maximum transmission unit (MTU) of 1280 bytes required for IPv6. The 6LoW-PAN [8][10] adaptation layer gives this particular aspect by transmission of IPv6 packets over 802.15.4. and this 6loWPAN implements mechanisms for the packet seggreagation and reassembling, apart from the other different functionalities. The routing concerns by using the organization goals and policies. The Constrained Application Protocol (CoAP) [12] backs the communications at the application layer. This Protocols are currently designed at IETF to provide the interoperability .

B. Link Layer Protocols

Link layer protocols basically determine how the data is sent over the networks physical layer or medium. The Hosts on the same link will exchange the data using these protocols. It also determines how the packets are coded and signaled by the hardware device over the medium to which the host is attached. Some of the link layer protocols are as follows: 802.3 Ethernet: 802.3 which represents a collection of wired Ethernet standards for the link layer

802.11 Wi-Fi: 802.11 represents collection of WLAN standards. These standards basically provides the data rates from 1 Mb/s to 6.75 Gb/s Different standards operates with different data rates which are as follows

802.11a - Wireless network bearer operating in the 5 GHz ISM band with data rate up to 54 Mbps.
802.11e - Quality of service and prioritization
802.11f - Handover
802.11g - Wireless network bearer operating in 2.4 GHz ISM band with data rates up to 54 Mbps.
802.11h - Power control
802.11i - Authentication and encryption
802.11j Interworking 802.11k - Measurement re-porting
802.11n - Wireless network bearer operating in the 2.4 Ghz and 5 GHz ISM bands with data rates up to 600 Mbps.
802.11s - Mesh networking
802.11ac - Wireless network bearer operating be-low 6GHz to provide data rates of at least 1Gbps per second for multi-station operation and 500 Mbps on a single link.
802.11ad - Wireless network bearer providing very high throughput at frequencies up to 60GHz.
802.11af - Wi-Fi in TV spectrum white spaces (often called White-Fi).
802.11ah - Wi-Fi using unlicensed spectrum below 1 GHz to provide long range communications and support for the Internet of Everything.

802.16- Wimax: 802.16 represents collection of wireless broadband standards. These standards provides the data rates from 1.5 Mb/s to 1 Gb/s, for mobile stations provides data rates of 100 Mbits/s

802.15.4- LR WPAN: Low rate Wireless Personal area networks, provides data rates from 40 Kb/s -250Kb/s. These standards basically provides low-cost and low speed communications for the power constrained de-vices

2G/3G/4G - Mobile Communications: Based on the different generations of mobile communication standards IOT devices can communicates over cellular net-works data rates varies with different generations.

C. Network/ Internet Layer Protocols

This layer is responsible for transmitting the information or the data from source to destination ,by performing the host addressing and packet routing. The host identification can be done by hierarchical IP addressing schemes such as IPv4 or IPV6.

1) *IPV4:* Most deployed Internet protocol which is basically used for identifying devices in the network using hierarchical scene me uses 32 bit address scheme which allows 232 or 4,294,967,296 addresses. No guaranteed delivery
2) *IPV6:* Successor of IPV4 uses 128 bit scheme which allows 2128 or 3.4 * 1038 addresses.
3) *6LowPAN:* 6LowPAN (IPV6 Low power wireless Per-sonal Area Networks) which brings IP protocols to the lower power devices that have limited processing capability, operates on 2.4GHz frequency range and provides data rates of 250 Kb/s . These protocols also define compression mechanisms for IPV6 datagrams.

D. Transport Layer Protocols

These transport-layer protocols are responsible for the complete delivery of message transformation. The capability of message transfers can be set up on connections using TCP by handshaking or without acknowledgement as in UDP.

1) *TCP:* TCP is basically a Connection oriented protocol, ensures guaranteed delivery, provides error detection capability, avoids duplicate packets, provides flow control, congesting control to avoid congestion collapse improvises networks performance.
2) *UDP:* UDP is connectionless , basically used for the time-sensitive applications which have small data units for exchange ,UDP is considered as transaction oriented and stateless protocol .Does not provide any guarantee on delivery and ordering of data transmission and even does not provide guarantee on duplication.

E. Application Layer Protocols

Application layer protocols basically define the how the applications interface with the lower layer protocols to send the data over the network. Application layer protocols enable process-to process connections by using the ports.

1) *HTTP:* Hypertext transfer protocol is a stateless protocol and, the protocol basically follows a request response model, each http request is independent of the other requests. HTTP uses universal resource identifiers to identify http resources.
2) *COAP*: Constrained Application protocol is designed to M2M(machine) applications. The CoAP is a online transmission protocol for usage with constrained nodes and constrained networks in IOT. The protocol is designed for M2M applications such as smart energy and building-automation . CoAP runs on connectionless-UDP rather than connection-oriented-TCP, uses Client server architecture for transmission.
3) *WEBSOCKET*: Web socket protocol uses full duplex communication over single socket connection to ex-change the messages between client and server. It basically uses TCP, the stream of messages is sent between to and fro between client and server and the connection is kept open. Client can be an IOT device, browser or any mobile application.
4) *MQTT*: Message Queue Telemetry Transport relays on publish-subscribe model, it is a light weight messaging protocol. It uses client server architecture where client is an IOT device connects to server (MQTT broker) and then publishes the messages to topics on the server. The broker forwards the messages to clients subscribed to topics. The broker forwards the messages to the clients by subscribing to the topics. MQTT is suitable for limited processing devices and when the network bandwidth is low
5) *XMPP*: Extensible Messaging and Presence Protocol (XMPP) is used for communication in realtime and streaming XML data between network entities. XMPP covers wide range of applications like data syndication, messaging, gaming, multiparty chat and voice/video calls. XMPP is considered as decentralized protocol which supports two way communication between client and server. XMPP allows communication between dif-ferent IOT devices.
6) *DDS*: Data Distribution Service (DDS) is a middleware standard considered as data-centric which is basically used for device to device communication or machine to machine communication.DDS basically uses publish subscribers model, the topics were created by publishers for which subscribers can subscribe .The publisher is basically an object which is responsible for the distribution of data and subscriber is responsible for receiving published data. DDS pro-vides quality of service control and also configurable reliability.

IV. SECURITY RISKS

There are different types of security risks which rises several doubts or concerns on IOT devices usage which could also be used to calculate the risk factor (1) Unprevileged access of resources and the misusage of personal information; (2) transforming attacks on

other systems; and (3) Extensively creating the safety risks. Although most of these kinds of risks exist with conventional systems and networks, they are more heightened in the IoT device.

A. Realtime Risks

According to recent statistical and other survey reports of IOT zone three types of applications might be vulnerable to security threats webcams, patient monitoring and smart vehicles . Majority of hackers or technological activists public and private cams all over the world .There are different tools like shodan.io which gives the provisions for the average tech users to access remote webcams. Second type of risk is of patient monitoring IOT not only enables the monitoring of medical equipment but also the users Experts, advised that the malicious hackers can access equipment to speed patients heart rates up. Also, drug in fusion pumps can be modified to alter the amount of morphine or antibiotics provided to the patients. In the third. case smart vehicles like smart cars, cycles are highly vulnerable and can be run under only on predetermined paths, as the traffic parameters changes with different countries based on the area, location and people the smart vehicles are highly vulnerable and considered as a realtime risks. Hayder A. A. Al-Kashoash [20] proposed a algorithm to avoid congestion control in 6LoWPAN networks which may lead to denial of service attacks, they proposed a novel approach called game theory based on the congestion control framework-GTCCF specially framed for the congestion control in 6LoWPAN networks. This framework could be considered as one of the best solutions to avoid congestion control intact solves the problem of denial of service attack when attackers try to insert more no of packets in the path to make congestion and stopping the service. The limitation of this algorithm is it could only serve to avoid the congestion

V. CLASSIFICATION OF IOT ATTACKS

The Previous works have done comprehensive studies on IOT security they have provided the taxonomy of IOT attacks and mentioned few solutions for different types of attacks. They are as follows. Andreaet al. [13] came up with a taxonomy of IoT devices attacks, and gave the classification in four distinct types: 1) the-physical; 2)the-network; 3) the-software; and 4)the-encryption attacks. The-physical attack is the attack done when the attacker is in a approximate distance of the device. The-network attacks are the type of attacks which is done based on manipulations done in network like modifying route allocation tables etc. The software attacks are the type of attacks that happen due to vulnerable aspects in code, these type of vulnerabilities are done intentionally by the developers or unknowingly which give attacker to introduce malicious activities into system. Encryption attacks are the attacks done to break the high-level-protection. These type of various-kinds of attacks can be attempted by guessing techniques, brute force techniques, side channel, cryptanalysis, and man-in-the-middle attacks. As per the different studies made [21] to defend the security concerns or problems at the physical layer, the devices should have a secure-booting by application of advanced hash algorithms and also digital signatures to verify its source by authentication and integrity of the service. Before the transmission of data any device with in the network has to authenticate itself in the network , it should also carry error detection system ,to maintain data integrity and confidentiality the information should be encrypted. Point-to-point encryption could be used at the network layer to ensure the privacy of the data and routing security.. The application layer could also provide security by means of identity authentication, encryption, and verification which allows only authorized users to access the data using control lists and firewalls.

A. Side channel attacks

Side channel attacks are the attacks by which attacker's gains information by using the physical implementation of the system. For example some IOT devices reveal information about the power consumption of the device, location, sound etc, which can provide extra source of information to the attackers that can be exploited to break the system. As an example Collusion attacks [22], some of the IOT devices manufactured by the same developers which run by using different type of applications or API's seek the permissions acceptance by the user to run the applications on the devices. Permissions may be of different types like location, sharing of contacts, sharing of External storage memory etc .As most of the applications which have their entire code embedded in the XML files. For example considering smart phone or other different smart devices which have user interfacing running under android applications may store the entire code in XML manifest files, by using the intent filter options if the different applications have been released by the same developers then they may share UID of the devices knowingly or unknowingly, which makes provision to the collusion attacks occur .It is one of the challenging issue in IOT security. One more issue arises where unauthorized access to CC cameras raises potential physical safety concerns. Likewise unauthorized access of data collected by fitness and other devices which tracks the consumers location over time. An-other type of issue is that a thief would remotely access the data about the energy usage from smart meters to determine whether a homeowner is away from home or not and based on that the theft done can be decided by thief.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor :6.887
Volume 6 Issue I, January 2018- Available at www.ijraset.com

VI. APPLICATIONS OF IOT

The idea of IOT, with its vision of network-associated objects with different abilities and form factors, could help the part of ICT (Information and communication Technologies) and as advancement empowering agent in an assortment of utilization markets. we distinguished six applications which are treated as IoT innovations health-care, environmental monitoring, smart homes/smart building, smart cities, Smart business/Inventory and product management and security and surveillance.

A. Healthcare

The no of applications in the healthcare sector use IoT technologies for various detections, report generations etc. The medical sensors were carried along with patients to monitor different parameters of body temperature, blood pressure, breathing activity, pulse detection etc. Other types of sensors are also used to continuously monitor the patient activities in the living environments. The required-data stored is locally transmitted through remote-locations by using different connectivity's where the medical treatment can be made easy for the doctors by using such type of devices. Even most of the sensors today are used to keep track of a person's daily activities .where they can know the calories burned, exercises performed etc

B. Environmental monitoring

Continuous Real-time-data processing, combined with the ability of large no of devices to communicate among them, gives a solid platform to detect and monitor anomalies or inconsistencies which leads to endanger the human and animal life. In another sense the IOT tech, can able to the detection of fire accidents and iceberg collision detection by using the devices which could help the environmental conditions. The agencies like INCOIS (Indian National Centre for Ocean Information Services) use sensors for the tsunami detection all over the world. Many other IOT technologies can be used to detect earthquake detections, environmental disasters etc.

C. Smart Homes/Smart Buildings

Adapting buildings with cutting edge IOT innovations may help in both decreasing the utilization of assets related to: structures (power, water) and in enhancing the fulfilment level of people populating it, be it labourers for office structures or inhabitants for private houses. Impact is both in money terms and additionally societal ones. In this application, a key part is played by sensors, which are utilized to both screen monitoring and in addition to that proactively recognize current clients' needs. Such a situation integrates no of subsystems, and hence requires a high level of standardization to guarantee interoperability.

D. Smart Cities

IOT devices can be utilized to provide advance traffic control systems. By using IoT devices in cars it is be possible to monitor heavy traffic in cities which avoids congestion in traffics or highways. The parking space are for the cars can also be known by using smart car parking systems where RFID sensor used to detect the vacant area in the parking area easily and show the information to the car driver/owner so that parking can be done easily. The average speed a car should travel can also be detected by sensors based on the type of road ,based on the type of person driving the car the smart systems in the car can give an alert on speed that reduces the accidents.. Nowadays many developing countries like India are concentrating more towards making more smart cities all over the country by implementing above mentioned techniques and other different techniques as a result there is a lot of scope for the researchers to work under this area .

E. Smart business/Inventory and product management

RFID innovations are now utilized as a part of numerous segments for stock administration, all through the supply and conveyance chain. This depends on the capacity of RFID innovations to recognize and offer help for following goods. At the occasion, notwithstanding, RFID applications are worked in a fairly specially appointed manner, and are just some-what integrated into supply administration frameworks..

F. Security and surveillance

Security reconnaissance has turned into a need for big business structures, shopping centers, industrial facility floors, auto parks and numerous other open spots. Country security situations faces additionally comparative dangers, but on an alternate scale. IoT-empowered advancements can be utilized to enormously upgrade the execution of current arrangements, giving less expensive and less intrusive contrasting options to the boundless organization of cameras while in the meantime safeguarding clients' security. Encompassing sensors can be utilized to screen the nearness of perilous chemicals. IOT technologies can provide high level of security control by providing basic security goals. Access control mechanisms are designed in such a way that thorough monitoring

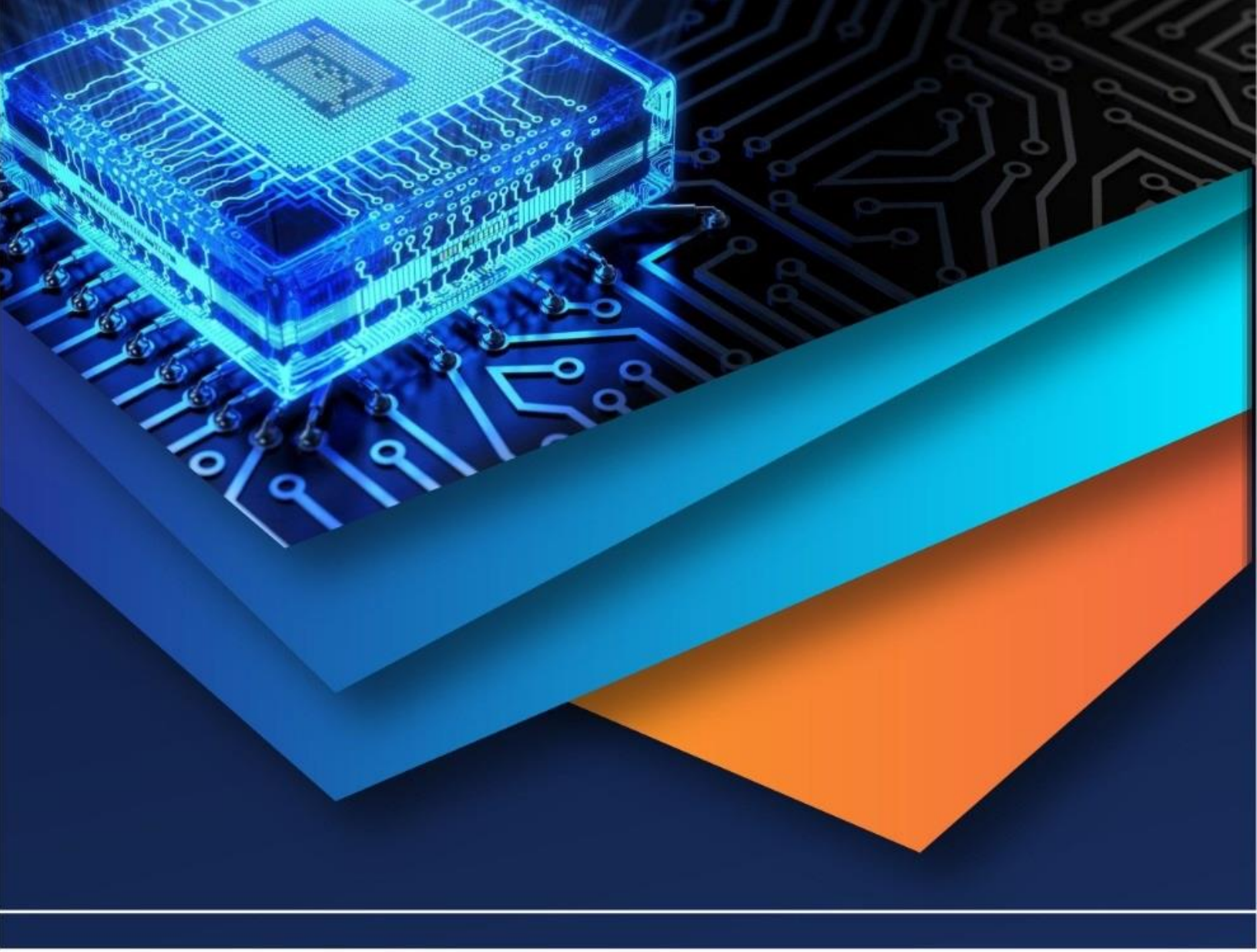
can be done. There are certain kinds of IOT devices like sensors where the timely access control can be given automatically and even it accessing of information changes with taking location parameters into consideration also.

VII. CONCLUSION

In this paper we summarized the IOT (Internet of things), it's importance in present era, the layers in the IOT .We have given a clear description of the types of protocols used in different layers. By considering different evaluations done previously, we summarized security risks with IOT devices, IOT security attacks, Applications of IOT and its usage and finally concluded.

REFERENCES

[1] O.Vermesan, P. Friess, P. Guillemin et al., Internet of things strategic research roadmap, in Internet of Things: Global Technological and Societal Trends, vol. 1, pp. 952, 2011.
[2] I. Pea-Lpez, Itu Internet Report 2005: The Internet of Things, 2005.
[3] I. Mahal, O. Alsaryrah, T.-Y. Chung, C.-Z. Yang, W.-H. Kuo, and D. P. Agrawal, Choices for interaction with things on Internet and underlying issues, Ad Hoc Networks, vol. 28, pp. 6890, 2015.
[4] O. Said and M. Masud, Towards internet of things: survey and future vision, International Journal of Computer Networks, vol. 5, no. 1, pp. 117, 2013.
[5] M. Wu, T.-J. Lu, F.-Y. Ling, J. Sun, and H.-Y. Du, Research on the architecture of internet of things, in Proceedings of the 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE '10), vol. 5, pp. V5-484V5-487, IEEE, Chengdu, China, August 2010.
[6] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, Future internet: the internet of things architecture, possible applications and key challenges, in Proceedings of the 10th International Conference on Frontiers of Information Technology (FIT '12), pp. 257260, December 2012.
[7] H. Ning and Z. Wang, Future internet of things architecture: like mankind neural system or social organization framework? IEEE Com-munications Letters, vol. 15, no. 4, pp. 461463, 2011.
[8] M. Weyrich and C. Ebert, Reference architectures for the internet of things, IEEE Software, vol. 33, no. 1, pp. 112116, 2016.
[9] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, Internet of Things (IoT): a vision, architectural elements, and future directions, Future Generation Computer Systems, vol. 29, no. 7, pp. 16451660, 2013. F. Bonomi, R. Milito, P. Natarajan, and J. Zhu, Fog computing: a platform for internet of things and analytics, in Big Data and Internet of Things: A Road Map for Smart Environments, pp. 169186, Springer, Berlin, Germany, 2014.
[10] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, Fog computing and its role in the internet of things, in Proceedings of the 1st ACM MCC Workshop on Mobile Cloud Computing, pp. 1316, 2012.
[11] I. Stojmenovic and S. Wen, The fog computing paradigm: scenarios and security issues, in Proceedings of the Federated Conference on Computer Science and Information Systems (FedCSIS '14), pp. 18, IEEE, Warsaw, Poland, September 2014.
[12] M. Aazam and E.-N. Huh, Fog computing and smart gateway based communication for cloud of things, in Proceedings of the 2nd IEEE International Conference on Future Internet of Things and Cloud (FiCloud '14), pp. 464470, Barcelona, Spain, August 2014.
[13] L. Atzori, A. Iera, and G. Morabito, SIoT: giving a social structure to the internet of things, IEEE Communications Letters, vol. 15, no. 11, pp. 11931195, 2011.
[14] IOT devices topic in IOT hands on approach by arshdeep bahga and Vijay madisetti
[15] Website::http://www.radio-electronics.com/info/wireless/wi-fi/ieee-802-11-standards-tutorial.php IoT Protocols
[16] Website :http://coap.technology/
[17] Website :https://xmpp.org/
[18] Website :https://techbeacon.com/4-stages-iot-architecture
[19] Hayder A. A. Al-Kashoash : "Congestion Control for 6LoWPAN Networks:A Game Theoretic Framework , IEEE internet of things journal, vol. 4, no. 3, june 2017
[20] Ioannis Andrea, Chrysostomos Chrysostomou," Internet of Things: Security Vulnerabilities and Challenges, The 3rd IEEE ISCC 2015 International Workshop on Smart City and Ubiquitous Computing Applications 978-1-4673-7194-0/15/$31.00 ©2015 IEEE
[21] M. Kireet ,Dr.Meda Sreenivasa rao,"Investigation of Collusion Attack Detection in Android Smartphones "(IJCSIS) International Journal of Computer Science and Information Security,Vol. 14, No. 6, June 2016
[22] Andreas Zankl, Hermann Seuschek, "Side channel attacks in IOT" –chapter 13 in Solutions for Cyber-Physical Systems Ubiquity book published by IBI Global
[23] IOTZONE Website : https://dzone.com/articles/iot-security-risks- real-examples



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY