Journal of Advances in Science and Technology
Vol. 17, Issue No. 1, March-2020, ISSN 2230-9659

A Study the Technology and Architecture of Internet of Things (IoT)

Balendra Kumar Garg[1]*, Dr. Vijay Singh[2]

[1] Research Scholar, Shri Krishna University, Chhatarpur M.P.

[2] Associate Professor, Shri Krishna University, Chhatarpur M.P.

Abstract - The Internet of Things (IoT) is the network of physical items like mobile devices, home appliances, vehicles, buildings and any other objects which are implanted with electronics, software, sensors, and network connectivity that empowers these objects to collect and interchange data. The IoT makes objects to be sensed, recognized and controlled remotely through the existing network infrastructure. This property creates opportunities for the incorporation of the physical world into the computer-based systems and subsequently improves efficiency, accuracy and economic benefit; when IoT is combined with sensors and actuators, it becomes an example of cyber-physical systems, which also incorporates technologies such as smart grids, smart homes, smart cities and intelligent transportation systems. IoT is a new era of communication which involves various objects and communication technologies to interchange information.

Keywords - Internet of Things, Technology, Architecture, Security, Application

----------X----------

INTRODUCTION

Internet of Things (IoT) is the concept that refers to a system of physical objects including mobile devices & home appliances which are integrated with electronics, software & sensors that facilitate these devices to gather & exchange information. Because of the Iot, any existing network infrastructure can detect, recognize, & control remote objects. For example, when sensors and actuators are used in conjunction with IoT, it becomes an example of a cyber-physical system that also incorporates technologies like smart grids, smart homes, smart cities, & intelligent transportation systems. Because of the embedded computing system, each item can be uniquely identified while also interacting with the Internet's existing infrastructure.

IoT does not have a singular definition. any services can be provided by the IoT over the IoT by enabling communications between humans & things, things to things and things to things, and machines to machines (M2M) (Singh et al. 2018). A human, a sensor, a device, or potentially anything else that can request or provide a service is a heterogeneous object in the IoT model (Atzori et al. 2016).

The 'IoT' concept is difficult to define because it differs from one field of study to the next. When it came to coming up with an official definition of the IoT, several different organisations& research teams contributed their ideas. The basic idea is that the IoT will connect the electronic, electrical, & non-electrical objects that surround us in order to present seamless communication & contextual services provided by them. The development of RFID tags, sensors, actuators, & mobile phones has made the IoT a reality, allowing the service to be improved & made available at any time and from any location. Working Group on Internet-based Systems Engineering. Every item in this sensor-enhanced web is linked together IET (Institute of Engineering & Technology)

INTERNET OF THINGS ARCHITECTURE

In IoT, there is a critical need for an architecture that provides scalability, flexibility, interoperability, & reliability for the communicating devices.

IoT architectures have included the three-layer [Yang 2017], the four-layer SOA service-based and the five-layer [Khan 2017] architectures shown in figure [1]. We'll go over each of these listed in the following section.

Five Layers Architectures

1. Perception layer:

It is the bottom layer of the IoT architecture, which is called the perception layer (also known as the sensing or object layer). Smart devices such as sensors, RFID, 2D-barcode, actuators, etc. are used to communicate with physical devices & components. Everything in an IoT network is connected through the perception layer, which not only handles identification but also measures,

collects, and processes data about things like temperature, humidity, location, motion, and other such variables as these. Layer interfaces are used to transfer the processed data to the next layer.

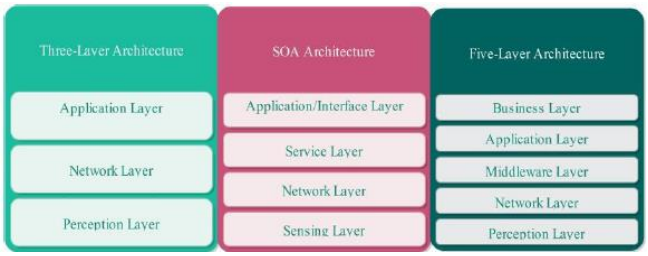

Figure 1: IoT Architectures

2. Network layer:

The transmission layer is another name for the Network layer. IoT devices & applications are securely routed to IoT devices & applications via integrated networks by the network layer that receives processed information from the perception layer. Wireless and wired communications technologies contain ZigBee or Bluetooth and PLC & LTE all play a role in the network's operation. Messages are sent from the network layer to the middleware layer.

3. Middleware Layer:

In between the networ & application layers, the middleware layer exists. Processing and filtering of information is done through this method. Only devices that implement the same service type can be connected to and communicate with by each other. Additionally, this layer is linked to the database for service management. When the network layer sends information to the database, it receives it.

4. Application layer:

The middleware layer transmits object information to the application layer, which then uses it to manage all of the applications & services they require globally. Additionally, the application layer provides services to a variety of applications, including storing data in a database, and analysing data received from physical devices to predict how they will perform in the future. Many different applications run at this level, each with their own set of specifications. Examples include smart homes, smart grids, smart agriculture, smart transportation, smart cities, and so on [Al-Fuqaha 2017].

5. Business Layer:

IoT system activities are managed by this layer, which includes the applications & services. The data received from the application layer is used to build business models, graphs, flowcharts, and so on. To further enhance services and protect user privacy, this layer analyses the data outputted by this layer. The outcome of this layer's analysis will guide the company's future actions & business plans.

IOT ENABLING TECHNOLOGIES

IoT is made up of a variety of technologies. IoT is built on these foundations today. Identification, localization, sensing, & IP address provisioning technologies, as well as technologies enabling small devices to communicate with other internet entities, will be needed to handle the expected massive influx of devices. Some of the most important IoT enablers are discussed in this section.

Radio Frequency Identification

RFID is a key enabler of the IoT. An RFID device, also identified as an RFID tag, is required to connect and communicate with small objects, as well as provide real-time tracking. You can identify & track objects by attaching an antenna to a microchip with a built-in antenna. Reading data stored in RFID tags does not necessitate a line-of-sight between the RFID reader and the tag.

Internet Protocol Version 6 (IPV6)

The number of IoT devices that will be connected in the future is enormous. The current 32-bit IPV4 addressing format supports 4.3 billion exclusive IP addresses. As a result of addresses being overloaded, the expected billions of IoT devices will be unable to connect. IPV6 was develop to increase the number of available IP addresses by providing 3.4 x 1038 addresses, which is enough to identify each object in the IoT situation [Ma, Jianguo 2017]. All of the network's devices can now be assigned an IPv6 address. There should be a unique identifier for each device on the network.

Wireless Sensor Networks

These days, WSNs use sensor nodes that can "feel" (collect physical data) and "think" (process data & make informed decisions) as well as a wireless channel to "talk" (communicate with other entities). Embedded in objects, these sensor nodes collect data about their surroundings, includes temperature, humidity, and motion of those objects. In order to take action based on this information, sensor nodes could be used to make electronic and non-electronic objects (such as food items & cars) aware of their surroundings. Smart refrigerators, lights, & locks, for instance, can let you know if food is running low and alert you accordingly. Sensors bring things to life and make them aware of the world around them.

IPv6 Low Power Personal Area Networks (6LoWPAN):

Because IPv6 requires a packet size of at least 1028 bytes, but IEEE 802.15.4 only allows packets of 128 bytes, the Internet Engineering Task Force (IETF)

developed 6LoWPAN, an adaptation layer between the IP stack's link & network layers that allows IPv6 datagrams to be transmitted over IEEE 802.15. 6LoWPAN, on either side, has classified a set of protocols and mechanisms, including encapsulation & compression RFC 6282 RFC 4919, RFC 4944[Fernandes 2016], that enable the integration of IoT devices into IPv6 networks.

IOT APPLICATIONS AND NEED FOR SECURITY

Aspects in the IoT are meant to be accessible at any time and from any location. IoT has helped to open up a extensive range of new and diverse application & service areas. Figure [2] shows a wide range of IoT applications & services, which will be discussed in the following sections.

Figure 2: Internet of Things Applications

Smart Homes

Home automation refers to the process of transforming everyday home appliances into technologically advanced systems that can be managed and controlled from a distance over the internet. Remote control of smart home appliances, such as refrigerators & washing machines as well as light bulbs and air conditioners, makes life easier and more comfortable [Li, Shancang 2016].

Wearable Devices

Smartwatches, fitness bands, & smart glasses are examples of small, intelligent devices with sensors & wireless connectivity that are being used to track people's health & activities throughout the day. Some interesting applications include those that help disabled people, such as the connected insoles that help blind people navigate by vibrating their shoes in the desired direction instead of using a screen.

Smart Cities

"Smart cities" are defined by the integration of various technologies, including smart housing, intelligent transportation, intelligent environmental monitoring, intelligent energy, & intelligent governance. Smart garbage receptacles, for example, have sensors & connectivity that allow employees to get real-time information about the status of those receptacles so that they can respond quickly to keep a city clean.

Smart Healthcare

Remote monitoring of patients and the elderly can be improved by integrating IoT technologies with medical devices. For example, pacemakers integrated with IoT technology allow medical practitioners to access real-time data on patients' cardiovascular readings. This revolution in treatment and disease diagnosis improves early detection of illnesses. In this way, they can be alerted immediately if the IoT devices detect abnormal heart activity [Catarinucci 2017].

Smart Agricultural

Farmers can monitor soil & crop health with small sensors & actuators to increase crop productivity or use resources like water efficiently at a lower cost. By 2024, the numeral of linked agricultural devices is predictable to raise from 13 million to 225 million, as per a Machina Research statement in 2016[Elijah 2018].

Energy Management

IoT aims to develop energy efficiency & reduce waste. We can learn a lot about energy use and waste by looking at the data, and we can also get a better idea of how much energy we'll need in the future. Utilizing sensors, these lights can respond dynamically to changes in the surrounding environment, resulting in a significant reduction in energy consumption.

Smart Transportation and Connected Cars

Using an intelligent transportation infrastructure, vehicles, the cloud, & traffic monitoring centre can communicate seamlessly to ensure safe, convenient, & efficient travel. Real-time navigation, automatic signal control (ASC), and other services are all part of smart transportation [Sherly 2017]. Vehicles are connected to each other in an ad hoc manner in the vehicular network.

WIRELESS SENSOR NETWORKS

WSN consists of finite sensor devices which are dispersed geographically usually in an indoor or outdoor predefined environment. The objective of WSN is to collect environmental data and the location of the nodes may be previously known or unknown a priori. Nodes in the network actually communicate with all devices and based on the application such communication describes a mesh or star topology. However, this differs from case to case. Depending on the roles of the node, it may be ad hoc or strategy based on the available resources in the network (Singh *et al.* 2016)

Power capacity for processing depends on the device, hence centralized formation techniques are appropriate for WSN. Here, the task of the device is to process, coordinate and manage the activities of sensed information and then transmits these data to sink node. But with distributed formation, every node manages the information and decisions are made locally which are limited to its single-hop neighbors. Recently used distributed techniques is self-organization. The process of forwarding information is complex and hence robust techniques are required. The network with this strategy achieves a promising behavior where nodes individually communicate and coordinate independently (Schmeck*et al.* 2016). Naturally, those techniques are involved in colonies of insect, birds flock, biological cells, ant foraging behaviour and so on.

Block Representation of Wireless Sensor Node

Sensor node has four primary elements namely sensing,processing, transceiver and power units are in Figure 3. Additional components that are dependent on the application include location finding, mobilizer and power generator. ADCs (analog to digital converters) and sensors are the two subunits of sensing units (Akyildiz*et al.* 2016). Analog signaling for the sensors, which will be sent to the processor unit, is converted by ADC to digital. The Storage Unit processing unit generally manages the processes that integrate sensor nodes with other nodes to perform the assigned sensing tasks. Connect the node to the network is part of the receiver unit.

Power unit is the main element of the sensor node that supports power supply units such as solar cells. The remaining subunits are request-based. Modular methods of design provide a versatile and flexible platform to meet the demands of different applications. The device is replaced or reprogrammed by sensors, which enable multiple sensors are act as wireless network node. Through radio access compliance also eliminated with wireless range specifications and device bidirectional communication.

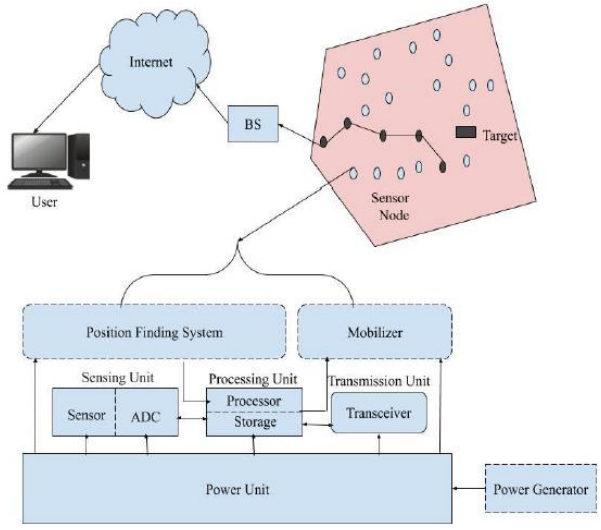

Figure 3: Components of a sensor node

Types of Wireless Sensor Networks

Various types of WSNs based on environment is constructed those are:

- Terrestrial
- Multimedia
- Underground
- Mobile, and
- Underwater

WSN

As per the network topology, WSN is constructed based on mesh network with multi-hop scenario. To transmit data and routing it uses Ad hoc On-Demand Distance Vector (AODV) protocol; hence nodes can be located anywhere within the network provided wireless link exists to communicate. These links are dynamically created as well as refreshed. Universal Serial Bus (USB) connects the sink and gateway.

Gateway Server

This is the key component which extracts Wi-Fi frames. By replacing suitable frame headers, Wi-Fi frames are transformed to Zigbee frames which is then sent to sink. These Zigbee frames with IP packets are encapsulated in USB frame. This component has the responsibility to receive and transform IPv4 packets to IPv6 and vice versa. The other role is to forward the sensor data received from WSN to middle-ware. Here, when the connection is lost between gateway server and middleware, the former stores the received data temporarily and then forwards to the latter when the link is gained.

Middle-ware

This is a software component which masks the heterogeneity feature thus making it translucent to the external users. Moreover, it automatically controls and reduces the energy consumed. The major roles are reception of data, filtering, storing and transformation of data in comprehensible manner for reducing utilization of energy. Further, this component provides an interface through web services to the end users for accessing the required information and to control appliances via WSN (Mikhaylov*et al.* 2016).

Mobile client

This is deployed in Android mobiles which helps users to consume energy at their homes in real-time. Additionally, the appliances are controlled remotely by turning them On and Off. During On or Off, the mobile client sends a direct command to the node which has to control the appliance.

SECURITY IN WSN-IOT

As WSN has a prospective future, it will be successful only when security and privacy issues are addressed. These are more significant as used generally in crucial applications. Moreover, WSNs are very vulnerable to attacks as the cost is very low for deployment (Roman *et al.* 2016).

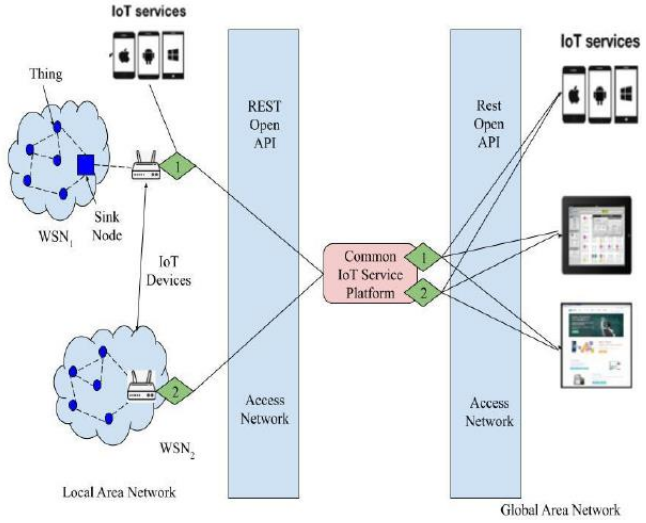

Figure 4: WSN-IoT security service platform

Figure 4 depicts the general requirements of IoT security platform and REST open API to construct WSN-IoT applications. WSN1 denotes a legacy system where sink is connected with IoT device having Internet connectivity and WSN2 is a WSN system enabled with IoT. Both WSNs are linked with common service platform such that every data and function of any type of WSNs are controlled by IoT applications through REST open APIs. Various security requirements for IoT layers are presently briefly in Table 1.

Table 1: Security requirements of various IoT layers

IoT LAYERS	SECURITY REQUIREMENTS
Application	• Data reduction is application-specific • Privacy and Policy Management • Authorization, Authentication, Assurance • Encryption and cryptography to be application specific
Services support	• Managing data must be protected and operations like data processing, searching, aggregating, correlation and computation has to be handled efficiently in a secured way • Cryptographic approach to store data
Network layer	• Sensor/Cloud Interaction must be Secure • Cross-domain Data Security • Secure Communication and Connectivity
Smart object/sensor	• Controlling node access • Lightweight Encryption • Format as well as Structures of data • Trust Anchors and Attestation

Types of IDS

IDS are classified into two as follows (Raoof*et al.* 2019).

- Host based IPS (HIPS): This is a package installed in the system for monitoring single host for the sign of malicious on going activities (Wazid*et al.* 2017).
- Network based IPS (NIPS): This detects and prevents various attacks in the network by monitoring the whole network to identify malicious traffic by analyzing various on-going activities

HIDS is designed for a single system for protecting the system from intrusions or malignant attacks thereby preventing the attacks of operating system or data. Generally, HIDS are dependent on host environment like log files in a system which is the input to HIDS decision engine. Thus, for any HIDS the primary task is to extract features from the host environment. NIDS sniffs the traffic packets of the network for detecting intrusions along with malicious attacks which can either be hardware or software based system. For example, FPGAs (field programmable gate arrays) are the building blocks for hardware-based NIDS. Special features of FPGAs like supporting high-speed interfaces, reprogramming dynamically and processing huge volume of data, makes FPGAs popular and suitable to use in NIDSs.

Intrusion Detection Techniques

Algorithms developed for IDS must be efficient such that they are implemented at various stages of detecting intrusion. Among several algorithms, few are briefly discussed. Misuse-based intrusion detection technique utilizes signature database, malignant code patterns as well as intrusions for detecting popular attacks. Packet overload, expensive signature matching, more false alerts are the major disadvantages of this approach. Moreover, severe constraints related to memory in few networks were the reasons for the low performance of this technique. Further, in signature-based and pattern-matching IDSs, signature as well as pattern databases has to be updated constantly. These approaches detects malicious attacks and intrusions with the prior knowledge on it.

In anomaly-based IDS, with the data of the normal users, normal data pattern is generated which is then compared online with current patterns for detecting anomalies. These anomalies are mostly due to noise or phenomena having the probability of creation with the hacking tools. Hence concluded that anomalies are not normal behaviors and are then initiated by the intruders which leaves footprints in the computing environment and are detected for identifying especially the unknown attacks. This IDS creates a model with normal behavior which is updated constantly and this model can be used for detecting the deviation of normal behavior.

APPLICATION OF WSN-IOT

WSN-IoT is applied in vast range of applications which impacts on human life for reducing human life simple and monitoring daily activity of human. Hence, many applications with WSN-IoT domains emerged. Figure 5 provides few promising applications associated with WSN-IoT environment.

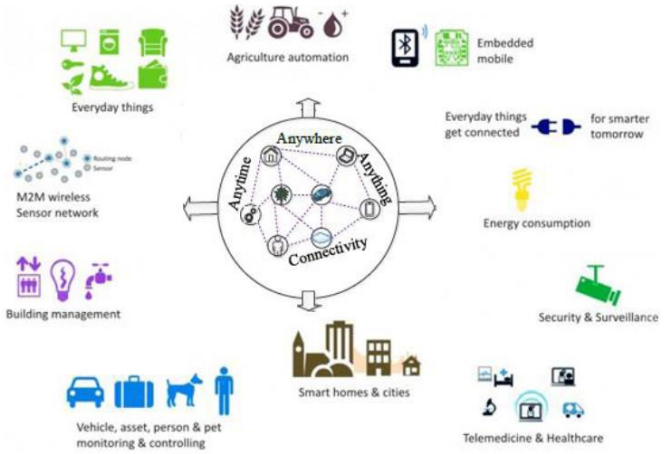

Figure 5: Applications of WSN-IoT

Home automation: IoT is mostly well-suited with any type of devices. In home appliances, IoT introduces smart automatic system. Users are able to control home from remote area using IoT home automation system. These provide more support for elderly people. Moreover, their children help them to control home appliances using smartphones.

Monitoring air pollution: Air pollution is usually is a common issue nowadays. Dangerous particles like led, sulphur dioxide, carbon monoxide and few other heavy particles are also included in the polluted air. Further degradation is caused in the air quality especially in metro cities. This pollution leads to dangerous diseases like asthma, Chronic Obstructive Pulmonary Disease (COPD), reduces the functioning of lungs, mesothelioma, Pneumonia and pulmonary cancer.

Monitoring Smart health: Life of human nowadays are very stressful and no proper care related to health is taken. Generally no regular checkups are made. For example IoT related smart health monitoring systems provides a solution for all these problems. Health sensors embedded in the human body senses the level blood pressure, sugar, heartbeat or whatsoever it may be and sends a notification immediately to the doctor is abnormal.

Smart traffic management: Usage of vehicles has increased and thus issues related to traffic occurs in almost all areas. WSN-IoT based smart traffic management system resolves this issue. This system has inbuilt smart sensors which communicates with one another. The information of these vehicles are sent to the cloud server which are further used for prediction.

Detecting and avoiding flood: Flood, a natural disaster, is commonly seasonal by which several countries suffer. It leads to economic crisis and even human lose their lives. Hence, flood has to be predicted earlier to save lives and property thus the idea of developing a system for early flood detection have aroused. This is achieved by measuring the level of temperature, humidity, water and flow. Float and flow sensor monitors the water and flow level respectively.

Smart anti-theft: Security is the major concern in the society. Every human need security at home or company. WSN-IoT based applications overcomes this issue. When a user is out of the house, turn on the antitheft system which monitors the footsteps on the floor tiles and sends alert if an intruder is at home. This is achieved by the sensor deployed and activated.

Safety system for coal mines: Coal mine is continually under risk of lives as it is a dangerous place where worker easily lose life. Hence researchers planned to develop a safety system for coal mines which utilized Arduino device to interface the microcontroller with gas as well as temperature sensors. If the gas sensor finds that the level is higher than the desired one then an alert is given to the corresponding authorities regarding the harm that will be caused due to the gas level. Hence, lives of the workers at coal mine can be saved.

Smart agriculture: AS the population increase worldwide, farming is more important to feed the population. Hence new techniques has to be used to increase the production with IoT framework. Agriculture is affected due to terrible weather conditions, sudden change in climate and some factors based on the environment of the land. IoT based smart farming helps farmers to increase the productivity and reduce wastage. Smart farming is a process with hi-tech low cost system for cultivation. Here, the crop field is monitored with the sensors which observed the illumination, temperature, soil moisture and irrigates automatically.

CONCLUSION

Internet of things (IoT) is a fastmoving collection of internet-connected sensors embedded in a wide-ranging variety of physical objects i.e. things. Whereas things can literally be any physical object (animate or inanimate) on the planet, to which you could connect or embed a sensor. Sensors can take a large number of possible measurements. Internet connectivity to the things can be either wired or wireless. Objects can be of any thing which must exist physically i.e. animate and inanimate. Security and privacy in IoT still a hot research topic. It attracted a lot of research interest in the past few years. IoT network is formed with resource constrained and low-power low-performing objects.

REFERENCES

1. Abomhara M., and Koien, G. M., "Security and privacy in the Internet of Things: Current status and open issues", in Privacy and Security in Mobile Systems (PRISMS), International onference on IEEE, 2017, pp. 1-8.

2. Abomhara, M. and Køien, G.M., 2017, _Security and privacy in the Internet of Things: Current status and open issues', In Privacy and Security in Mobile Systems (PRISMS), 2017 International Conference on pp. 1-8, IEEE.

3. Abomhara, M., &Køien, G. M. (2017). Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. Journal of Cyber Security and Mobility, 65-88.

4. Adafruit – datasheet, 2017, _ESP8266 wifi chip', Available: https://cdn-shop.adafruit.com/product-files/2471/0A-ESP8266 Datasheet EN v4.3.pdf

5. Adat, Vipindev, and B. B. Gupta, "Security in Internet of Things: issues, challenges, taxonomy, and architecture", Telecommunication Systems, Vol. 67, Issue 3, 2018, pp.423-441.

6. Addo Ivor D., Sheikh I. Ahamed, Stephen S. Yau, and ArunBuduru, "A reference architecture for improving security and privacy in internet of things applications", In Mobile Services (MS), International Conference on IEEE, 2017, pp. 108-115.

7. Agrawal, Shashank, and Dario Vieira. "A survey on Internet of Things." *Abakós*1.2 (2017): 78-95.

8. Ahmed Mohammed Ibrahim Alkuhlani and S.B. Thorat"Internet of Things (IoT) Standards, Protocols and Security Issues" International Journal of Advanced Research in Computer and Communication Engineering 4.11 (2017): 491-4952017.

9. Airehrour David, Jairo Gutierrez, and Sayan Kumar Ray, "Secure routing for internet of things: A survey", Journal of Network and Computer Applications, Elsevier, Vol. 66, 2016, pp.198-213.

10. Akyildiz, I.F., Su, W., Sankarasubramaniam, Y. and Cayirci, E., 2016, _Wireless sensor networks: a survey. Computer networks, vol. 38, no. 4, pp. 393–422

11. Ammar, Mahmoud, Giovanni Russello, and Bruno Crispo. "Internet of Things: A survey on the security of IoT frameworks." *Journal of Information Security and Applications*38 (2018): 8-27.

12. Ammar, Mahmoud, Giovanni Russello, and Bruno Crispo. "Internet of Things: A survey on the security of IoT frameworks." Journal of Information Security and Applications38 (2018): 8-27.

13. Andrea, I., Chrysostomou, C. and Hadjichristofi, G., 2017, _Internet of Things: Security vulnerabilities and challenges. In Computers and Communication (ISCC)', IEEE Symposium on pp. 180-187, IEEE.

14. Andrea, I., Chrysostomou, C., &Hadjichristofi, G. (2017, July). Internet of Things: Security vulnerabilities and challenges. In 2017 IEEE symposium on computers and communication (ISCC) (pp. 180-187). IEEE.

15. Arshad, J., Azad, M. A., Amad, R., Salah, K., Alazab, M., & Iqbal, R. (2020). A review of performance, energy and privacy of intrusion detection systems for IoT. Electronics, 9(4), 629.

16. Atkinson, Randall, and Stephen Kent. "Security architecture for the internet protocol." (2016).

17. Atzori Luigi, Antonio Iera, and GiacomoMorabito, "The internet of things: A survey", Computer networks, Elsevir, vol. 54, Issue 15, 2016, pp. 2787-2805.

18. Bude, Cristian, and Andreas KerveforsBergstrand. "Internet of Things: Exploring and Securing a Future Concept." (2017).

19. Miorandi, D, Sicari, S., De Pellegrini, F. and Chlamtac, I., 2016, _Internet of things: Vision, applications and research challenges', Ad hoc networks, Vol.10 No.7, pp.1497-1516.

20. Miorandi, Daniele, Sabrina Sicari, Francesco De Pellegrini, and ImrichChlamtac, "Internet of things: Vision, applications and research challenges", Ad hoc networks, Vol. 10, Issue 7, 2016, pp.1497-1516.

Corresponding Author

Balendra Kumar Garg*

Research Scholar, Shri Krishna University, Chhatarpur M.P.