IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol.-6, Issue-11, Nov 2018 E-ISSN: 2347-2693

A Survey Paper on Internet of Things and its Data Security Issues

Krishna Priya Gurumanapalli[1*], M. Nagendra[2]

[1,2]Dept. of Computer Science and Technology, Sri Krishnadevaraya University, Anantapur, Andhrapradesh, India

[*]*Corresponding Authors: priya.racharla@yahoo.com*

Available online at: www.ijcseonline.org

Accepted: 25/Nov/2018, Published: 30/Nov/2018

Abstract- Data is the driving force in this modern digital era. There are numerous platforms available to send a data from one place to another through computer networks. This survey paper classifies and describes the network classification based on topology, connectivity, and geographic area. A brief introduction on Wireless Sensor Network (WSN) and Internet-of-Things (IoT) has been detailed based on the research. These two technologies are identified as a platform for data processing through different sensors. The data sent through the network using different platform contains all kinds of sensitive information. It is the responsibility of the technology providers to build suitable security systems that assure data privacy. This research paper has focused on a detailed investigation of the Internet-of-Things (IoT) and its data security. Different techniques used for data security are listed, among them, an Encryption technique is found to be effective and well suitable for IoT. This research paper presents the survey of some encryption algorithms. Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Rivest-Shamir-Aldeman (RSA) encryption techniques are briefed.

Keywords- Internet-of-Things (IoT), Data security, Wireless Sensor Network (WSN), Encryption.

I. INTRODUCTION

A. Introduction to Computer Network

A computer network is defined as a set of computers which are connected to each other in order to share information. These computers are connected through communication channels. One of the oldest computer networks isreported in the United States. Networks provide a wide variety of applications; helps to facilitate communication through email, audio, video, and instant chat. A computer network allows single device or resource to be shared among multiple users. The operating system can be shared with a remote computer through a network.The applications of the network are presented through different types of network. Network types are classified based on topology, connectivity, and geographic area. Network in terms of its topologies is classified into star topology, bus topology, ring topology, and mesh topology. In star topology, the devices are connected to each other devices through central node. In bus topology each device in the network is connected through a common cable, when device A has to send information to device D, the information sent has to traverse through the device B and C. In ring topology the devices are connected in a circular format, in this kind of network formation, information flows until it finds the intended recipient. The devices in a network are connected to each other in a mesh format, it is referred as a mesh network; in this kind of topology a device can send a message to the intended device directly [1].

A computer networkcan be classified based on the geographic area as Local Area Network (LAN), Wide Area Network (WAN), Metropolitan Area Network (MAN). LAN is a kind of network where it is allowed to communicate with devices within a building or an office. In WAN the devices are allowed to cover a large geographic area such as city, country, or an entire world. The MAN network allows devices to connect within a city.

The network formed between the devices can be connected either through wired or wireless medium. The network classification in terms of connectivity can be divided into wired network and wireless network. If the devices connected either through wired or wireless medium, the functionality remains same. Based on the client requirements the network is formed. Each type of network has its own advantages and limitations. In comparison with a wired network, it is found that wireless network is more efficient and convenient.

Further wireless network is classified into wireless stations, access points, and an ad-hoc network. Wireless stations allow devices such as mobile phones, desktop, laptop, etc. to be connected through a common network as shown in figure 1. One good example for this kind of network is a wireless hotspot.

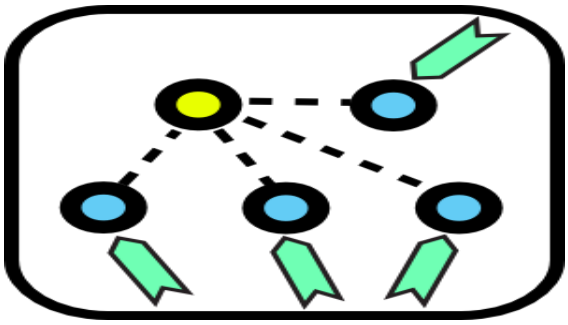

Figure-1 Wireless stations [1]

Access point wireless network hosts and manages the connections for devices as shown in figure 2. One example for the access point is Wi-Fi.

The Ad-hoc network allows devices to communicate directly without anything else in between as shown in figure

3. Ad-hoc network devices are connected without any access point between them. The ad-hoc approach applies its applications in terms of communication model in IoT and WSN.

Hence each device must use the same configuration to contribute. Wireless Sensor Networks (WSN), Internet-of-Things (IoT) are the best examples for this kind of network.

WSN are used for gathering information regarding the environmental changes. IoT is

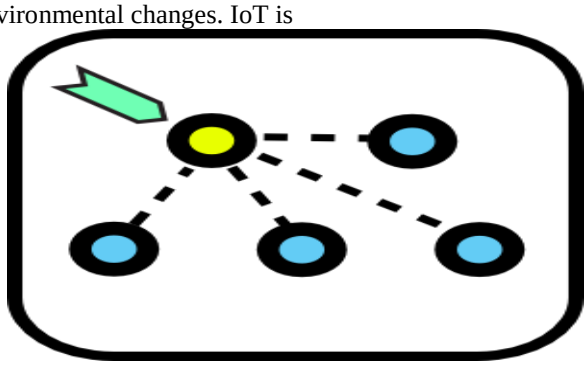

Figure-2 Access Points [1]

used for communication without the intervention of human and any other devices.

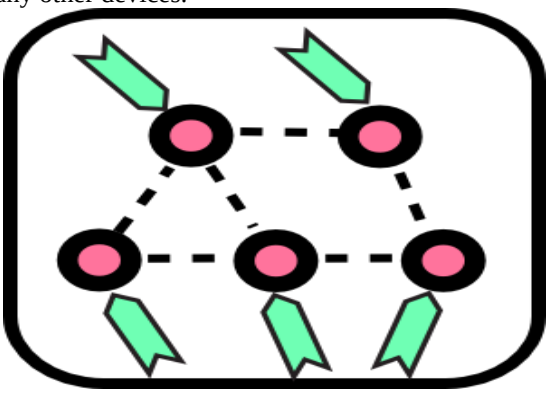

Figure-3 Ad-Hoc Network [1]

B. Introduction to WSN

Wireless Sensor Networks (WSN) is one of the most widely used technologies of this era. WSN can be referred to as a distributed network of sensor nodes spread over the geographical area. WSN is an advanced type of network and a successor of the traditional network which evolved after the introduction of wireless communication protocols. It is an area of profoundly networked systems of low-power wireless nodes that comprise an insignificant amount of memory and CPU and also large federated networks intended for highresolution. In addition to that WSN devices are equipped with sensors and communication unit. The sensors in WSN have a capability to sense the environment and transfer the information to the base station. WSN can include various types of sensors like vibration sensors, temperature sensors, magnetic sensors, bio sensors, and chemical sensors. Sensors log the change in the event and information will be fed into processing unit. The processing unit will intimate processors to execute different tasks [2].

The performance of WSN is evaluated through sensor node characteristics. They are: Fault tolerance – eachnode in the network should not incline to an unexpected error, fault tolerance is the ability to preserve sensor node without any node failures. Communication failure – If the nodes in the WSN failed to transfer the message to other nodes, it is required to inform the nodes without any delay. The flexibility of nodes – Thenodes in the network have the capability to move independently across the network. Node assortment – Thenodes in the WSN require various varieties of nodes. Scalability – Thenodes in the network can be scaled up based on the application; nodes can be from a hundred to thousands. Network topology- The nodes in the network should follow standard topology and must have the ability to work in dynamic topology. Independence – WSN is independent in nature it does not have control point. The impracticability of public key cryptosystems –Thelimited power and computation of sensor nodes frequently result in undesirable conditions to use the public key. Sensor utilization – Sensorsshould be utilized in such a way that it produces a maximum performance with minimum energy [3].

Most of the WSN protocols are designed for two-way communications, but naturally, it is required to send and receive information to the sensors. In order to introduce two-way communication in sensors, an Internet-of-Things was introduced. For instance, implementation of WSN in smart grid enables the system to keep track on energy production and consumption in order to improve the energy usage. WSN will not let the system to perform any actions to reduce the consumption of energy. By implementing IoT in smart grid, it enables the system to provide information regarding the energy consumption, execute the smart algorithms and communicate with related devices through the internet to optimize the energy usage. IoT has become

familiar and widely accepted as it replaced the manually operating activities to automatic operations. Due to these significant functionality differences, WSN was overhauled from IoT [4].

WSN applications created a huge impact on various fields because cost of WSN devices is minimal. The sensor node is the main part of the WSN; these sensor nodes can obtain the environmental changes. In order to identify and meet market trends, IoT was introduced. The small inexpensive and low powered WSN has integrated into IoT, which created a major evolution in WSN. WSN does not require any complex infrastructure, and it spends less energy as the devices will be in sleep mode to conserve energy.

C. Introduction to Internet of Things (IoT)

In the 2000's, We are heading in to a new era of ubiquity, where the users of the internet will be counted in billions and where the human may become the minority as Generators and Receivers of Traffic. Instead, most of the Traffic will flow between devices and all kinds of things, thereby creating a much wider and more complex internet of things. Usage of the Internet of Things (IoT) is Increasing at a rapid amount and expanding its importance for professionals to understand regarding its functionality, applications, and its impact on businesses. IoT can be defined as the association of uniquely recognizable embedded computing devices within the environment of the internet. Advanced levels of services can be offered with the help of IoT based technology. The different things like Light, Table, Chair, The watch like anything and everything that you can think of, all these are going to be fitted with embedded systems, Embedded electronics and Information Technology so that they have some basic computing platform in them attached to them then they are going to be acting as different nodes of that particular internet the IoT.

Embedded system basically comprises sensors, input, Processors, microcontroller, memory speed, Communication systems,controllers, and a display unit. Through this embedded system can control the devices and home appliances. Devices that are connected to the embedded system and embedded system to the internet helps to access and control generated data in sensors. The devices included in IoT setup can connect to the internet through Wi-Fi, Ethernet, Wireless cellular technology, blue -tooth,Zig bee and the different technologies that are available to us.All these embedded systems connected to other things depending on the application requirement and the specific goals of the business and then a big internet is going to be formed [5].

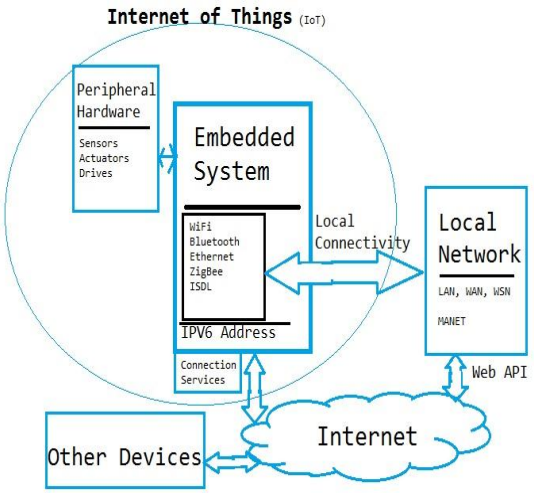

Figure-4 IoT architecture [5]

The architecture of IoT comprises hardware boards, Application Program Interface (API), protocols, software systems all these components creates a unified environment as shown in figure 4. This seamless environment allows embedded devices to connect to internet autonomously.

There are different enabling Technologies for IoT[6]. Example RFID(Radio frequency identification) uses radio waves to identify items. The track items in real-time to yield important information about their location and status. Sensors-Sensors bridge the gap between physical and virtual worlds and enabling things to respond to change in the environment generating information and raising awareness about the context. Micro controllers-These are computer chips that are embedded in to objects. It empowers things and devices in the network to take independent decisions. Protocols-Machine to machine interfaces and protocols of electronic communication set the rules engagement for two or more nodes of a network. Biometrics-Biometrics enables technology recognize people and other living things, rather than inanimate objects. Machine vision-This is an approach that can monitor objects having no on-board sensors, controllers or wireless interfaces. Actuators-Actuators detect an incoming signal and respond by changing something in the environment. Location Technologies – These help people and machines find things and determines their physical whereabouts. Some things translate their own radio, light and sound inorder to disclose their whereabouts to people and machines. The devices are connected to the internet through different protocols like Wi-Fi, Ethernet, and so on. The devices in IoT are addresses in the IPv6 scheme. By assigning devices of IoT with a unique IP address can make it discoverable on the internet as an autonomous node.

The Internet of Things has many advantages it can able to connect both non-living and living things. So what is going

to happen is because the number of things is very large, much larger than the number of computers that are available, so it is going to increase the number of nodes in this particular network. So IoT in other words is going to have large number of nodes, each node corresponding to the different distinct objects that exists in the physical world. The purpose of IoT has expanded to connect every object from an everyday object to industrial tools. Generally, any object that is embedded with sensors and has connectivity to the internet that can participate to communicate with other devices can be referred to as IoT.

IoTis one of the building blocks that is considered to be of use for developing smart phones and smart cities so at present not only In our country but throughout the world there is a lot of internet in developing smart cities and smart homes. So IoT is one of the enabling technologies to make the city smart and to make the home smart. In the healthcare industry, IoT helps to track the location of the patient wheelchair to cardiac defibrillators. In this way, IoT helps to communicate with devices. The connected devices in the IoT require to control from remote places sometimes. Every now and then organization might require to turnon some devices remotely in order to perform some actions, in such case IoT helps to control the devices. With the implementation of IoT in an organization had helped to save money. Implementation of IoT has reduced the failure of equipment in the organization and has allowed to run operations smoothly without any interference and hence saves the organization money [7].

IoT has been contributed to its functionality in various fields, and however, the amount of data generated through the devices is huge. The huge amount of data has made organizations to look for an alternative that could reduce the risk of maintenance. Cloud computing technology has been the perfect solution for storage solutions in IoT. By storing the generated data in cloud allow IoT companies to access a huge amount of Big data. IoT's role is connecting devices is immense, but its ability would be incomplete without security. With the implementation of cloud in IoT has made more secure. Cloud computing with strong security measures like authentication and encryption has helped IoT to prevent any kind of threats. The integration of cloud computing in IoT has created a new revolution for organizations.

Applications of IoT

Some of the real-world applications in IoT are:

1. Smart home – Smarthome is a most associated feature of IoT. IoT revolutionized the world by replacing the manually operated devices for automated.
2. Associated cars – Anassociated car allows to optimize its own activities such as maintenance, operation, navigation using onboard and internet connectivity.
3. Smart city – Thepowerful application of IoT is a smart city. IoT will give solution for major issues that have been facing in many cities. The problems such as pollution, resources, energy management, traffic, etc. are solved through IoT sensors using web applications.
4. Wearables- Wearables have created evolution in the health industry. The devices are installed with sensors, and these sensors collect data about the users to extract insights. In addition to health, wearables can also fulfill the requirement in the field of fitness and entertainment.
5. Agriculture- Government has started helping farmers to use IoT to increase food production. To determine the fertilizer, sensing soil moisture and nutrients, controlling water usage, etc. are the simple uses of IoT [8].

IoT is more captivating, and it has been introducing in many fields' day by day. This technology is replacing manually operated activities into automatic.

Advantages of IoT over WSN

1. WSN offers one-way communication, whereas IoT provides two-way communication.
2. Sensors in WSN exhibit limited functionality, whereas sensors in IoT performs communication and controlling.
3. In WSN, sensors nodes are connected to the base station, in IoT sensor nodes can act as a base station.
4. WSN has limited networking capability compared to IoT.
5. WSN may or may not have cloud integration, but IoT has cloud integration.
6. WSN require a centralized controller (base station), which is optional in IoT.
7. Data processing (Big data, machine learning) can be implemented in IoT but not in WSN due to its limited functionality.
8. WSN is limited to sending sensory data, IoT includes actuation.
9. WSN has limited storage capacity,whereasIoT has unlimited storage (depends on the cloud).
10. WSN has limited applications, IoT applications can be extended to almost every field.
11. IoT has stronger data security because security can also be implemented through the cloud.

This paper is divided into four sections. The first section describes the introduction of Computer Networks, Wireless Sensor Networks and Internet of Things. Also it includes applications of Internet of Things and advantages of IoT over WSN. The second section discusses the current research activities in IoT and what are the data security issues present in the IoT. Privacy and security issues are discussed in the third section. In the last section, I concluded that AES, DES and RSA algorithms are implemented to IoT to make enhanced security by providing defense against the attacks.

II. RELATED WORK

A. Current research activities in IoT

IoT has become a reality, and it is found everywhere. This technology is revolutionizing the world and progressing to a new level. Now in recent times, IoT has stepped into the field of Toys. These toys allow to monitor children from remote places, and GPS tracker helps to find the lost toys. Teddy the Guardian is one of the IoT based toys, the sensor in the toys helps to check child temperature and heart rate instantly [9].

B. Data security issues in the IOT

One of the greatest challenges IoT is facing is data security while transmitting data seamlessly from source to destination it is necessary to hide from adversary attacks. Some of the most common attacks in IoTare Distributed Denial of service attacks (DDoS), unauthorized users, information leakage, and falsification.

DDoS- This is one the most hazardous attack, they infect the target devices by sending malicious codes and make them not function properly. In order to prevent from this kind of attack, it is required to implement authentication method.
Falsification- When IoT devices send information packet using application server the attacker might collect the packets. The collected data by an attacker can be misinterpreted or might leak the original content. It is required to block unidentified devices when it proceeds to access the IoT devices.

Unauthorized user- when an attacker tries to decode the security parameters of IoT devices, there may be a chance of failure of the present security system. The failure of the current security system might result in loss of the important data of a user. In order to avoid this kind of threat, it is required to implement with access control mechanism.

Information leakage- IoT comprises with a lot of sensors which could get hacked easily. As these sensors contain sensitive information, it is required to secure the user data. In order to avoid information leakage, it is essential to implement data encryption or user authentication mechanism must be instigated.

A world cannot be imagined without IoT, because everyone in today's world has been hooked to IoT directly or indirectly. As IoT is known for collecting data from devices, it helps business, organization, and industries to run more proficiently. Collecting a large amount of data is one big challenging task in IoT, and with a collection of data providing privacy is the biggest challenge. Researchers are working to come up with a brand-new system that could safeguard the user's information efficiently.

III. PRIVACY AND SECURITY

IoT has proved to be more efficient and has increased the profit rate in many organizations. With the growing popularity, IoT's security system requires to build stronger from the previous system. The connected devices in IoT include personal data and IP where a hacker can easily utilize these data. There are several techniques available to create a secure environment for data.

Authentication- In order to protect the devices from threats in IoT, it is required to check the identity of devices to seek the permission to access the data. To check the identity of the devices, an authentication technique is used broadly. In authentication technique sensors, gateway, device, and server identity is checked before it is involved in the communication process. As the devices of IoT have shortened lifespan, this authentication technique becomes a barrier, and it demands frequent authentication for the same device for several times [10].

Intrusion Detection System (IDS)- One more mostly used security technique is Intrusion Detection System (IDS). IDS system helps to detect the malicious activities in the network. It can also monitor the traffic and reports it to the administrator. This system makes administrator carry out required action to exploit the vulnerabilities. The extended solution of IDS is Intrusion Prevention System (IPS) which can be able to block the threat in addition to detecting the threat in the network. [10]. As IoT technology is vast and implementation of IDS/IPS security technique could not able to withstand the attacks. This kind of method is suitable for small applications.

Encryption techniques- This is one of the conventional methods of securing data. The process of converting original data into another format which an attacker could not understand is defined as Encryption. Encryption is widely used for different things but mostly used for data security. The data which is converted into the unrecognizable format is referred to as Ciphertext. There are two types of encryption available they are Symmetric and Asymmetric. In symmetric encryption same key is used for both encrypting and decrypting data. In case of asymmetric data, different keys are used for encryption and decryption method. The keys in asymmetric encryption are referred to as a public and private key. The public key is shared among many users for whom data is intended to be shared. The private key is shared with the authorized person, so when data is shared user can decrypt the data using the respective private key [11].

Hashing is one more technique of encryption that generates the fixed mathematical value out of the original message. Generally, hash functions are used with cryptography in order to provide digital signatures. The original text

converted to the hash value is difficult for hackers to retain the original information.

Through a detailed study, it is found that Encryption is the ideal solution for securing data. There are various reasons that prove why encryption technique is better than other data security techniques. Encryption provides a standard security mechanism for all information whether it is important or not. The data becomes venerable when it has to move from source to the destination location. For a skilled user, it is easy to corrupt the encrypted data by altering; encryption assures to maintain the integrity and help to retain original data. Encryption helps to protect sensitive data from attackers, by ensuring anonymity and privacy. For the organizations who have strict compliance to secure personal information, uses encryption technique to anonymize the information of the client. Regardless of the organization or company, encryption technique also protects the data from all devices.

Encryption Algorithms:

Encryption algorithms convert the original data into unrecognizable format and reconverts back to a readable format. There are several encryption algorithms are available, each algorithm exhibits different mechanism to secure data. This survey paper presents few commonly used encryption algorithms. Before that let's see the classification of encryption technique.

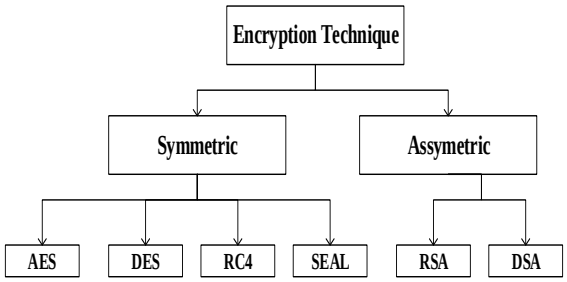

Figure-5 Classification of Encryption Technique [10].

Both symmetric and asymmetric encryption have different algorithms as shown in figure 5. This survey paper discusses on important encryption algorithms.

Advanced Encryption Standard (AES)- The strength of the algorithms is relied on its effectiveness in ensuring data security. Advanced Encryption Standard (AES) has an ability to replace the data of length 128, 192, and 256 and the algorithms are referred to as AES-128, AES-192, and AES-256 respectively. 128-bit AES algorithm will divide the complete text into four blocks, each block is considered as an array of bytes, and it is organized as an order of matrix. This AES-128 algorithm includes 10 rounds before they deliver final ciphertext. Each of the rounds performs four transformations they are sub-bytes, shift-rows, mix-columns, and add round key. In case of converting back ciphertext to original text also includes 10 rounds before it delivers final document and, in each round, it performs following functions they are inverse substitute bytes, inverse shift rows, and inverse mix columns [11] [12].

Data Encryption Standard (DES)- It is one of the widely accepted encryption algorithms. This algorithm was developed by IBM and has an ability to encrypt the data consisting of 64-bits. Though DES has input key of 64-bits long, actually used by DES is 56 bits. The algorithm transfers the 64-bit text in a series of steps in an output of 64-bit. This algorithm is broadly used in financial services and other sectors where it is required to protect sensitive information [13].

Rivest-Shamir-Aldeman (RSA)-This is one of the popular asymmetric types of encryption. This algorithm uses two prime numbers to generate public and private keys. The process includes three steps they are: key generation, encryption, and decryption. RSA is available in three different forms RC4, RC5, and RC6 [13]. The algorithms are compared and sown in table 1. It is clearly seen that Symmetric algorithm is more secure than an Asymmetric algorithm.

Table-1 Comparison of RSA, AES, and DES [11].

Factor	RSA	AES	DES
Bit length	Depends on the number of bits in the modulus	128,192, or 256 bits	56 bits
Cipher type	Asymmetric	Symmetric	Symmetric
Security level	Least secure	Exceptional secure	Not secure enough

IV. CONCLUSION

The use of network has been growing rapidly and also sharing data through the internet. With the growing requirement for network and internet need for data security is also increasing. The journey of computer networks, network types, WSN, and IoT has briefed in this paper. This paper emphasizes more on security techniques for IoT. To provide effective security technique, encryption methods are used. My contribution in this paper is a survey on encryption algorithms has been done; each algorithm has its own functionality and suitable for different applications. Through background research, it is found that AES, DES, and RSA are most commonly used encryption algorithms. The security mechanism of these mentioned algorithms can be enhanced further. These encryption algorithms are implemented to IoT to make enhanced security by providing defense against the attacks [14].

REFERENCES

[1] "Types of Wireless Networks | Commotion Wireless", Commotionwireless.net. [Online]. Available: https://commotionwireless.net/docs/cck/networking/types-of-wireless-networks/.[Accessed: 19- Jun- 2018].

[2] C. Cisse, K. Ahmed, C. Sarr and M. Gregory, "Energy efficient Hybrid Clustering Algorithm for Wireless Sensor Network", 2016 26th International Telecommunication Networks and Applications Conference (ITNAC), 2016.

[3] S. Zhang and H. Zhang, "A review of wireless sensor networks and its applications", 2012 IEEE International Conference on Automation and Logistics, 2012.

[4] N. Khalil, M. Abid, D. Benhaddou and M. Gerndt, "Wireless sensors networks for the Internet of Things," 2014 IEEE Ninth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 2014.

[5] D. Evans, The Internet of Things How the Next Evolution of the Internet Is Changing Everything. San Fransisco: Lopez, 2011, pp. 1-6.

[6]Paul Kirby, "Focus on FTC Staff Recommends Internet of Things Best Practices." Tele communications Report, Vol. 81,No.3,pp-3-3.

[7] B. Al-Shargabi and O. Sabri, "Internet of Things: An exploration study of opportunities and challenges," 2017 International Conference on Engineering & MIS (ICEMIS), 2017.

[8] S. Kashyap, "10 Real World Applications of Internet of Things (IoT) - Explained in Videos", Analytics Vidhya, 2016. [Online]. Available: https://www.analyticsvidhya.com/blog/2016/08/10-youtube-videos-explaining-the-real-world-applications-of-internet-of-things-iot/. [Accessed: 19- Jun- 2018].

[9] "Connected Toys and What You Need to Know About Them", Us.norton.com. [Online]. Available: https://us.norton.com/internetsecurity-iot-connected-toys-and-what-you-need-to-know-about-them.html. [Accessed: 19- Jun- 2018].

[10] A. Roney Mathew and A.Al Hajj, "Secure Communications on IoT and Big Data," Indian Journal of Science and Technology, vol. 10, no. 11, pp. 1-6, 2017.

[11]G. Singh and Supriya, "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security", International Journal of Computer Applications, vol. 67, no. 19, pp. 33-38, 2013.

[12]B. Daddala, H. Wang and A. Javaid, "Design and implementation of a customized encryption algorithm for authentication and secure communication between devices," 2017 IEEE National Aerospace and Electronics Conference (NAECON), 2017.

[13] M. Noura, H. Noura, A. Chehab, M. Mansour and R. Couturier, "S-DES: An efficient & secure DES variant," 2018 IEEE Middle East and North Africa Communications Conference (MENACOMM), 2018.

[14] A. Mamathashree, K. Remya and B. Kumar, "Fault analysis detection in public key cryptosystems (RSA)," 2017 International Conference on Communication and Signal Processing (ICCSP), 2017.

[15] R. Piyare and S. Lee, "Towards Internet of Things (IOT): Integration of Wireless Sensor Network to Cloud Services for Data Collection and Sharing," International Journal of Computer Networks & Communications, vol. 5, no. 5, pp. 59-72, 2013.

Authors Profile

Krishna Priya Gurumanapalli is pursuing Ph.D in Sri Krishnadevaraya Univerity, Anantapur, Andhrapradesh. She did Master of Computer Applications(M.C.A) from Sri Krishnadevaraya Univerity, M.Phil from Bharathiar University and M.Tech from Jawaharlal Nehru Technological University. She worked as an Assistant Professor in Intel institute of Sciences, Anantapur, Andhra Pradesh. Her area of research is on Computer Networks.

M. Nagendra, Professor,Department of Computer Science and Technology in Sri Krishnadevaraya University, Anantapur, Andhrapradesh. He is having 25 years of teaching experience in Computer science. He successfully guided 6 Ph.D students and currently 6 Ph.D scholars are doing research under his supervison. He published more than 20 international journals.His main research interests onComputer Networks and Software Engineering.

