Journal of Engg. Research Vol. 9 No. (2) June 2021 pp. 139-148` https://doi.org/10.36909/jer.v9i2.9823

The embedded framework for securing the Internet of Things

Feroz Khan A.B* and Anandharaj G**

**Department of MCA, C. Abdul Hakeem College of Engineering and Technology, Melvisharam, India.*
***PG and Research Department of Computer Science, Adhiparasakthi College of Arts and Science, Kalavai, India.*
**Corresponding Author: abferozkhan@gmail.com*

Submitted: 28/02/2020
Revised: 08/10/2020
Accepted: 15/10/2020

ABSTRACT

The smart devices connected on the internet turn to be the internet of things, which connect other objects or devices through unique identifiers with the capability of transferring and receiving the information over the internet. There are numerous applications in different areas such as healthcare, home automation, transportation, military, agriculture, and still so many sectors that incorporate cutting-edge technologies of communication, networking, cloud computing, sensing, and actuation. With this huge increase in the number of connected devices, a strong security mechanism is required to protect the IoT devices. Hence, it is required to focus on the challenges and issues of IoT enabled applications to safeguard the entire network from the outside invasion. This paper discusses some of the challenges in building IoT applications, a detailed study of the existing security protocols, and its issues, and the potential of the IoT.

Keywords: Internet of Things (IoT); Survey; Security.

INTRODUCTION

We live in the world of the Internet. Human life is changing day by day in the way you are using Internet resources. There has been a significant change in people's daily lives like using the Internet. Previously, we used to send letters by post, it takes a few days to reach the destination depending on the distance. But now, with the help of the Internet, we can send e-mails easily, which can be delivered to the recipient in a fraction of a second wherever recipient is. Many inventions have made the newspaper the routine of easy people. Even the Internet of things is one of those inventions which brought revolutionary change to the modern life of people. Internet of things is the interconnection of networks of devices in which data exchange, device access, and connection is via the Internet. Devices can be like a human being, a car, a mobile phone, a fan, etc., which are integrated with the sensors. To exchange data between devices, network connectivity is provided. IoT is one of the main research topics underway these days. There are many applications possible in the Internet of things as in fig 1. In today's digital life of people, there are many real-time applications of IoT. These include smart homes, smart cities, portable technology, smart farming, connected cars.

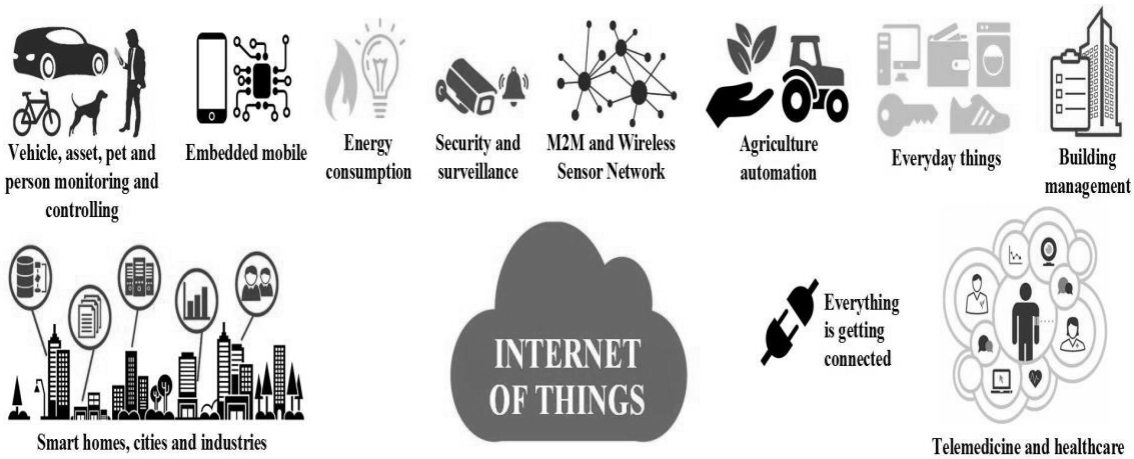

Figure 1. Internet of Things.

Smart City is a powerful IoT application that generates curiosity among the people of the world. The connected roads are the smart city core. Vehicle drivers can find parking spots easily without having to visit the city. The streetlights set with sensors can be used there. Air and noise pollution can also be controlled, and the water level in the rivers can also be controlled to avoid floods due to the use of sensors. Proper use of resources such as water and electricity can be carried out using the consumption data available in real time. Drivers can receive warning incidents and also suggest reduced traffic paths. Wearable technology is another technology that is creating voices in today's world. Portable devices include digital electronics with microcontrollers such as smart watches, activity trackers, which are IoT examples. They are mobile devices that can be used in the body as accessories. Activity trackers are used to track our activities, how far we have traveled, and how long we have exercised in our daily life, smart watches are portable devices that incorporate some features included in a smartphone.

(A. Jain, K. Kant and M. R. Tripathy 2012, Andrea, C. Chrysostomou, G. Hadjichristofi, 2015) Security plays an important role in any connected system. Also, in the IoT, there is a great requirement for security features. Like the devices in the IoT, the environment is heterogeneous. Therefore, it is very difficult to design required security features. In reality, the IoT defenses are very weak. Unlike mobile phones, desktops and tablets offer very little protection for IoT operating systems. There is also a reason for this. Because providing security to an IoT device can be expensive and may not be expensive to expect the desirable functioning of those devices, which leads to decrease in speed and capacity. In this paper, we examine the security issues and challenges of the IoT smart home. The remaining sections of the paper are as follows: Section II provides an overview of the IoT applications and the security challenges of IoT. Section III provides the embedded security objectives and challenges. Section IV consists of some possible directions of research to provide multilayer approach for the security of Internet of Things, and finally, the conclusion section.

Home Automation

The emergence of IoT devices at home can change our lifestyle by providing intelligent technologies with the help of sensors that communicate and are controlled remotely via the Internet. People with busy schedules can simplify their lives by connecting their mobile devices to the IoT device. Therefore, machine-machine interaction is possible without human intervention. Cloudwash is an example of IoT Washing Machine. You can connect your washing machine to the IoT, and you can control it from anywhere on your phone. You can also set the number of cycles needed to wash the phone. It is very useful for the person who wants to clean clothes when he comes home from the office. Another smart device is August Doorbell Cam, a beautiful IoT invention. August Doorbell Cam can answer your door remotely, constantly check your doors, and capture any change of movement at your door. The next IoT is WeMo Light Switch, it is used to manage the lights of the house through the wall, the mobile phone, or the voice. It is

connected to the existing Internet to provide wireless access to home lights. Nest Smoke Alarm is another type of IoT devices that is very useful for signaling any emergency from your home. It is used to detect smoke, it talks to you and warns you about what is happening at home. There are so many smart devices available on the market today, and the above list of smart devices is the best IoT device in the world.

IoT at workplace

Today's workplaces have become interconnected systems in which people work together with technology. At the workplace, the jobs and duties currently assigned are shared between employees and IT devices to achieve efficient business productivity.

Most Internet of Things (IoT) devices introduced in the workplace are small devices to manage the workplace more efficiently. For example, programmable energy strips are used in the workplace for advanced energy management on the Internet. It is used to switch appliances on/off from anywhere via the mobile phone or computer system. This will help the administration save energy resources by turning off all the devices when not in use (S. Kaedi, M. A. Doostari, and M. B. Ghaznavi-Ghoushchi, 2018). Another device that comes on the market notifies health professionals to inform them which garbage containers are full. This allows them to ignore the places where the containers are not full or empty, which reduces workers' time. Moreover, this will save fuel/gas and, therefore, time and money.

Implementing the IoT in the workplace is indeed a challenging task because the devices, employees, and devices are largely connected, and the devices must always be connected, and privacy protection is the most critical problem in other networks (J. Granjal, E. Monteiro, J. Sa Silva, 2015). However, the company can minimize costs if it effectively implements the IoT infrastructure. The Wi-Fi device connected via IoT is the main concern that nobody talks about, if companies provide high-speed routers like Wi-Fi-6, it can connect with multiple devices, and the speed of the devices can be much faster even in a busier network.

IoT at Healthcare

According to reports presented by P&S market research, from 2015 to 2020, there will be a compound growth rate of 37.6% in the health sector. Physicians can monitor the devices used to treat patients through the use of real-time location services. Devices used in the medical system such as scales, wheelchairs, nebulizers, defibrillators, monitoring equipment can be easily identified with the IoT by labeling them with sensors. Remote health monitoring also plays an important role in the health system. It can be used to treat patients remotely for those who cannot go to health centers every day like the elderly. There are also numerous useful health applications online.

IoT at Smart city

The smart city is composed of a variety of use cases, such as traffic regulation, waste management, distribution and control of water resources, environmental monitoring. IoT solutions in the smart city area can control waste management. It can be used to reduce traffic congestion by providing the best possible route for vehicle drivers. Noise and noise pollution of cities can be controlled by providing a threshold value.

IoT at Agriculture

Crops can be protected against deterioration due to animals through continuous monitoring. We can also control crop fertilization by maintaining accurate readings, electricity, and irrigation control. The health of animals they use for agriculture can also be controlled through monitoring and identification of the position of the animals that graze in open areas.

IOT RESEARCH CHALLENGES, THREATS, AND ISSUES

Although IoT is a technological advancement today, which gives lots of advanced services, it is at risk because of the various kinds of security assaults in our daily life. The important security violations are related to leakage of

confidential information and denial of services. The security assaults in the IoT environment directly damage the physical security of devices. The IoT consists of various kinds of computer devices and different platforms with different credentials, and every device connected in the network requires a strong security mechanism depending upon its characteristics (J. Granjal, E. Monteiro, J. Sa Silva 2015, Jhujhar Singh, Om Parkash, 2017). The user's privacy is a very critical concern here since their private information is being shared across various types of devices. Hence, strong security policies are required to protect private information (Feroz Khan and Anandharaj, 2020). Moreover, there are different kinds of devices connected in the network for providing IoT services, and communication among heterogeneous environments are also possible. Hence, there are lots of security challenges there, specifically on users' privacy and network layers.

Some of the critical security violations in the Internet of Things are as follows:

1) End to end protection: To provide complete security to the data travelling in IoT environment, end to end data protection can be provided to a whole network. The network can receive data from various devices outside the network, and the same can be shared across all the devices in the network. Thus, the network should have an efficient framework to protect the data from exposures, to preserve the confidentiality of data, and to manage information privacy in the full data life cycle.

2) Embedded security: The communication among the interconnected devices varies depending upon the situation. Therefore, the devices must have the capability of maintaining the security level in the device itself. For instance, the security policies implemented in the personal network for secure communication with sensor devices, and other smart devices should also be reflected in external communication with the devices outside the network.

3) Visible security and privacy: Most of the security and privacy concerns are invoked by the misconfiguration of users. It is very tedious to implement such critical privacy policies and security requirements. It is required to opt for security and privacy policies that are automatically applied and implemented in the environment.

FUTURE CHALLENGES

Internet of Things (IoT) is one of the important technologies in the era of digital transformation, everything on the planet can be connected to the Internet. It is the primary technology behind many smart things such as smart homes, driverless car, smart service counters, and smart cities. But there are lots of security challenges that we need to consider for the future of the Internet of Things (IoT).

The number of IoT devices is increasing rapidly in recent years. According to a company of Gartner analysts, by 2020, there will be over 26 billion connected devices worldwide, compared to only 6 billion in 2016.

Internet of Things provides effective communication between devices, they automate things, save time and costs, and offer many advantages. But still, one thing that concerns users is security. Many incidents happened that have made it difficult to trust IoT devices.

Many smart devices and ATMs have been breached, which is undesirably affecting not only consumers, but also companies. Therefore, the important security challenges are discussed below for the future of the IoT.

Regular updates

As the Internet of Things devices are increasingly used, device manufactures are aiming on building new devices alone, and they are not much concentrating on the security of the devices.

Most of the devices do not get regular updates. This means that these products are safe at the time of release, later it could be vulnerable to more attacks if the attackers find any security violations.

These kinds of issues can be resolved with the periodic release of updates for hardware and software. Otherwise, these devices can be vulnerable to attacks. Whatever the things connected to the internet, must be upgraded regularly to avoid security breaches. If regular updates are not done frequently, it can lead to data breaches to customers and manufacturers.

Week credentials

Most of the IoT companies, which sell their products, are providing customers with default credentials, such as an administrator username. Attackers only need the username and password to make assaults to the device. After knowing the username, they execute brute force attacks to perform some malfunctions.

The best example that can be considered for the reason of security violations, which uses default credential, is Mirai botnet attack. Default credentials should be changed by the consumer immediately after they get the device, this information must be given in the instruction unfortunately, it is not mentioned by many manufacturers. Failure to perform this update information in the instruction guides leads to different attacks.

Malicious activity

Since the growth of the development of IoT products are rapidly increased, it leads to permutations of cyber-attacks unpredictable. Cybercriminals are very advanced today, and they even prevent consumers from using their devices.

For example, a camera connected to IoT used to capture private information from home is hacked, and the intruders encrypted the surveillance system, and the original users are not allowed to access their required information. This way of attempting is called ransomware if the attackers ask the users to pay a considerable amount to recover their own data.

Prevention of attacks before it happens

Cybercriminals are well advanced and continuously discovering new techniques to break the secured system. So, it is very important to learn how to predict the attacks before it is executed in addition to fixing vulnerabilities.

The security challenge can be considered as a long-term challenge to provide security to the interconnected devices in IoT. To predict security in the cloud, threat intelligence are used in modern cloud services. Analysis and monitoring tools based on artificial intelligence are widely used predicting techniques today to predict the security of the system. However, it is very challenging to bring these techniques in the IoT due to the instant processing of each piece of data.

Difficult to find a device if hacked

One cannot expect 100% secured system against threats and security breaches, what happens with IoT devices is that most users do not know if their device has been hacked.

When the number of devices connected in the IoT are high, it is very hard to monitor security for the whole system even for the service providers. This is due to the nature of an IoT device, which requires applications, services, and communication protocols. As the number of devices increases exponentially, the amount of things that need to be managed increases even more. Therefore, many devices continue to work without the knowledge of users that they were hacked.

Data security challenges.

Data protection has become a really difficult task today in the millions of interconnected devices because the data can be transferred among multiple devices in seconds. In an instant, the data can be stored on the phone, the same is on the Web and then in the cloud.

Because all these data are traveled across the Internet, data loss can be occur anytime. (Feroz Khan, A.B et al., 2019) One cannot say that the data transmission is secure in all the devices where it is transmitted or received. Once the hackers find that the data is leaked, they can sell them to other companies that violate data privacy and security rights.

Furthermore, even if the data is not disclosed by the consumer, service providers may not comply with the laws and regulations. This can also lead to security incidents.

EMBEDDED SECURITY CHALLENGES

Since the embedded devices are increasing day by day and it is expected to be expanded even more, there is a need for critical security requirements to save the devices connected to the internet. The challenges for securing the embedded devices are considered in the following points.

Critical functionalities

Reliability and availability of devices should be maintained without interruption by performing all the required functionalities check. Authentication and identification of devices would be a challenging task if the critical functionality check is not proper (K. Rose, S. Eldridge, and L. Chapin, 2015).

Dependability

The primary principle of the dependency characteristic is that the system should be reliable and available. Other characteristics include maintainability, privacy, and protection of the system. Privacy is one of the major goals that the system should perform well even after system failure. Maintainability is also the vital requirement that the system should be highly adaptable for the upgrade of s/w and h/w.

Attacks

There are many alike devices constructed with similar designs and models like other devices connected in the atmosphere. If one of the devices becomes vulnerable, then all the security policies implemented in the system are questionable (Kalpana Sharma, M.K, 2010), and the violations can be replicated across the internet.

Infrequent patches

Frequent upgrade must be performed to maintain current security requirements. Because the IoT devices are dynamic in nature, security upgrade should be performed automatically from the remote system once the upgrade is released.

Security requirements

The security for the devices must be integrated into it right from the manufacturing of the devices until its life span to consider future security issues.

Deployment

Because the mobile devices can be placed outside the corporate perimeter, there would be a lot of security violations that might occur for the devices connected to the internet. Therefore it is necessary to address all the security challenges in order to safeguard the remote devices from various violations (Kumar, Sathish & Vealey, Tyler & Srivastava, Harshit, 2016).

EMBEDDED SECURITY OBJECTIVE AND REQUIREMENTS

Tamper resistance for the device, data, firmware, and communications are the important security requirements to be addressed. Figure 2 shows the security objective of IoT.

Securing data

The private data kept in the system should be encrypted and placed in such a way that it should be allowed only for authorized access. The primary concern is to combat both internal and outsiders attack by implementing strong securing policies. It is also necessary to use an efficient key management technique that the attackers should not have access to shared keys.

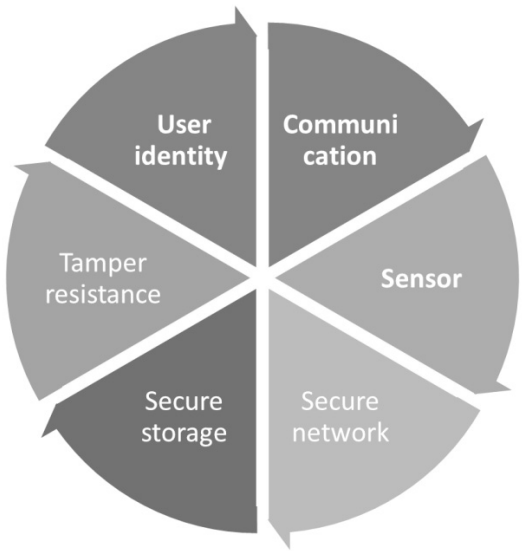

Figure 2. Security objective of IoT.

Booting security

The integrity of the manufacturer firmware implemented in the system and in the OS should be protected through secure boot. This secure boot will authenticate the firmware by verifying its digital signature before the operating system is started (S. Qiu, G. Xu, H. Ahmad, L. Wang, 2018).

Resistance to tampering

Tampering should be detected and prevented by the system internally. Antitempering technique must be implemented to prevent the data from alteration via any unauthorized channels either in transit or in storage.

Need for supervision

All the doings of the system must be monitored if there is any abnormalities found in the system. So, there is a need for implementing an efficient algorithm to find all the signed attacks and new attacks depending on the needs. Pattern matching is the most challenging task for detecting the patterns among all the available ones.

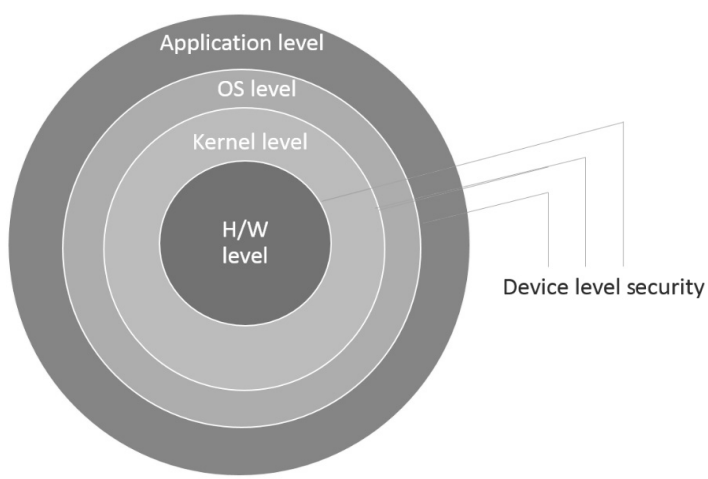

Figure 3. Embedded security requirements of IoT.

Secure Communication

The interception of data should be eliminated by protecting all the communications that occurred in the system. Authentication of sources should be performed efficiently to fulfill the basis of secret communication. This is used to ensure that all the communications happening between source and target are secret.

System security

Securing the network from outsiders is system security, and data security is the way of protecting the data stored in the system from attackers. The following are the common threats to the security of the system.

Backdoor: trapdoor or backdoor leaves the way to gain access to the system or any network resources violating the implemented security policies of the system. A backdoor could be implemented in the system to do the future modification or upgrade if any available in the future. Attackers might discover this backdoor, and they can penetrate the network to harm the system or data.

DoS: This attack prevents authorized access, and even the genuine user with access rights could not access the system resources. This attack can be done by transmitting unnecessary packets to the source once the source accepts the connection request. More number of request packets will be sent repeatedly by the attacker to make the system completely unavailable.

Side channel attack: If the attacker gains knowledge about the cryptographic technique used in the system, they will perform side channel attack. Different methods are available to perform side channel attack for the exploitation of private key.

Mal-ware attack: This attack will prevent access to legitimate users and have complete control over the target (J. R. Douceur, 2002). Later, the ransom will be demanded by the attacker to release their control over the target and to make it available to them.

The embedded security requirements to protect the IoT devices are shown in Figure 3. The embedded security provided to the application are shielded from the hw level, OS level, and kernel level. The embedded security refers to inbuilt security that provides device level security from the start the data entered into the device. Some of the security features required for embedded security are tamper resistance and encryption to perform authorization and authentication considering performance metrics such as reduced energy, time delay, and reduced computational cost.

IOT MULTILAYER SECURITY ANALYSIS

The researchers view about IoT architecture is given in Figure 4.

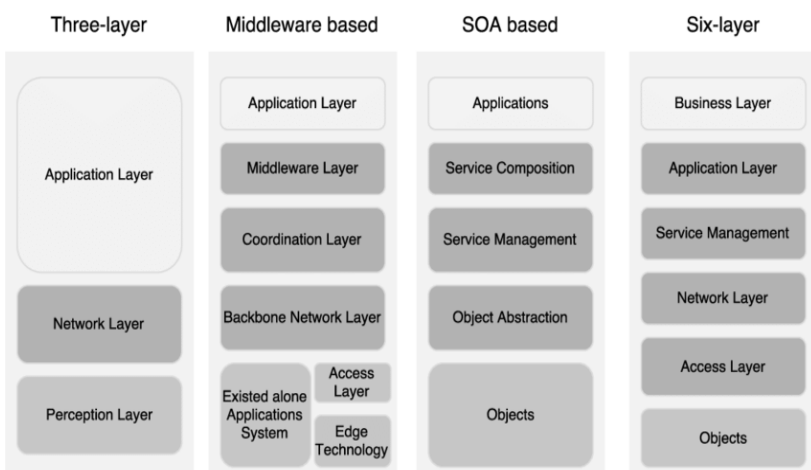

Figure 4. IoT Layered architecture.

Each layer in the IoT is prone to various kinds of security threats and attacks. The attack can be an active attack or passive attack, it can arrive from outside the network or inside the network, and multilayer approach can be used to prevent these threats. An active attack will straightaway block the service, while the passive will monitor the environment and eavesdrop the information without interrupting the service. Each layer in IoT are at risk of Denial of Service attacks (DoS), which is the most catastrophic attack that makes the service unavailable to even authorized users. The following sections present guidelines for the security requirements in each layer.

Table 1. Layer-wise security objective

Layer	**Security objective**
Physical layer	End device security
Communication/ transport layer	transport security
Objects layer	data security
Network Communication layer	Internet security
Cloud storage and data analysis layer	Cloud data security
IoT application layer	Application support security

CONCLUSION

Internet of things is the latest buzz word, which is largely increased in recent times. In this paper, we discuss some of the challenges and issues related to IoT security, and we proposed countermeasures for IoT smart environment, and the layer-wise security is analyzed. There are huge benefits and state-of-the-art facilities provided by the IoT based smart devices, but at the same time, there are so many security violations are possible which we should deal with. IoT security is the only critical issue which we need to consider to protect the IoT based smart environment. If strong security mechanisms and policies are implemented in the future to protect the IoT enabled devices, there will be a great scope in the future for the evolution of more numbers of IoT enabled applications which makes our life more convenient, fast, and secure.

REFERENCES

A. Jain, K. Kant and M.R. Tripathy 2012. "Security Solutions for Wireless Sensor Networks," 2012. Second International Conference on Advanced Computing & Communication Technologies, Rohtak, Haryana, pp. 430-433, doi: 10.1109/ACCT.2012.102.

Andrea, C. Chrysostomou, G. Hadjichristofi 2015. "Internet of Things: Security vulnerabilities and challenges", Proc. IEEE Symp. Comput. Commun. (ISCC), pp. 180-187, Jul. 2015.

Balijepalli, A., & Sivaramakrishan, V, Organs-on-chips: Research and commercial perspectives. Drug Discovery Today, **22**(2): 397-403.

Carsten Maple 2017. Security and privacy in the internet of things, Journal of Cyber Policy, 2:2, 155-184, DOI: 10.1080/23738871.2017.1366536R.

Daniel-Ioan Curiac 2016. "Wireless Sensor Network Security Enhancement Using Directional Ant ennas: State of the Art and Research Challenges", www.mdpi.com/journal/sensors2016.

Feroz Khan, A.B. and G, Anandharaj. 2020. "A Multi-layer Security approach for DDoS detection in Internet of Things", International Journal of Intelligent Unmanned Systems. https://doi.org/10.1108/IJIUS-06-2019-0029

Feroz Khan, A.B., Anandharaj 2019, G. "A cognitive key management technique for energy efficiency and scalability in securing the sensor nodes in the IoT environment: CKMT ". SN Appl. Sci. 1, 1575 (2019).

J. Granjal, E. Monteiro, J. Sa Silva 2015. “Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues”, IEEE Commun. Surv. Tutorials, 17 (3) (2015), pp. 1294-1312.

J.R. Douceur 2002. "The Sybil Attack," in 1st International Workshop on Peer-to-Peer Systems (IPTPS "02).

Jhujhar Singh, Om Parkash 2017. “A Survey on Wireless Sensor Network (WSN): Security Issues, Challenges and Solutions, Journal of Advances and Scholarly Researches in Allied Education” vol.14, no. 1, pp. 710 - 715 (6) 2017.

K. Rose, S. Eldridge, and L. Chapin 2015. “The internet of things: An overview,” The Internet Society (ISOC), pp. 1-50, 2015.

Kalpana Sharma, M.K 2010. Ghose, Deepak Kumar, Raja Peeyush Kumar Singh,Vikas Kumar Pandey. "A Comparative Study of Various Security Approaches Used in Wireless Sensor Networks". In IJAST, Vol 7, April 2010

Kumar, Sathish & Vealey, Tyler & Srivastava, Harshit 2016. Security in Internet of Things: Challenges, Solutions and Future Directions. 5772-5781. 10.1109/HICSS.2016.714.

S. Kaedi, M.A. Doostari and M.B. Ghaznavi-Ghoushchi 2018. "Low-complexity and differential power analysis (DPA)-resistant two-folded power-aware Rivest–Shamir–Adleman (RSA) security schema implementation for IoT-connected devices," in IET Computers & Digital Techniques, vol. 12, no. 6, pp. 279-288, 11 2018.

S. Kumar, S. Poddar, R. Marimuthu, S. Balamurugan and S. Balaji 2017. "A review on communication protocols using internet of things," 2017 International conference on Microelectronic Devices, Circuits and Systems (ICMDCS), Vellore, 2017, pp. 1-6.

S. Qiu, G. Xu, H. Ahmad, L. Wang 2018. “A Robust Mutual Authentication Scheme Based on Elliptic Curve Cryptography for Telecare Medical Information Systems”, IEEE Access, 6 (2018), pp. 7452-7463.

Vignesh, A.Samydurai 2017. “Security on Internet of Things (IOT) with Challenges and Countermeasures”, IJEDR , Vol.5, Issue 1, 417 – 423 ,2017.

Y. Xie and D. Wang 2014. "An Item-Level Access Control Framework for Inter-System Security in the Internet of Things," in Applied Mechanics and Materials, 1430-1432, 2014.