ENERGY EFFICEINT ROUTING PROTOCOLS BASED ON ZIGBEE TECHNIQUES

Pushpa Latha Thumma[1], Dr Prasadu Peddi[2]

[1]*Research Scholar, Department of Computer Science, Shri Jagdishprasad Jhabarmal Tibrewala University, Rajasthan*
[2]*Professor, Dep of CSE & IT, Shri Jagdishprasad Jhabarmal Tibrewala University, Rajasthan.*

ABSTRACT

Every day, new distributed computing systems make their way onto the market. Consequently, in developing these systems, new security and privacy issues come up. These difficulties necessitate the search for more thorough and accurate methods that can offer greater degrees of security, privacy, and confidence in these systems right from the start of their creation. To create systems, including open distributed systems, we require methods and resources for design, specification, and code creation. In order to facilitate understanding of the initial concepts of these systems, graphical notations are preferred. This is pertinent to the initial stages of design. After the concepts are settled upon, a formal foundation for the intended system's specifications is needed to enable critical thinking when it comes to designs and specifications. This can be completed in the final stages of design. Some of the security functionalities are missing from the existing documentation for security and privacy needs and functionalities in IoT systems. Specifically, privacy issues are either not addressed or are simply provided in textual form without a framework definition. In order to provide techniques that enhance the security, privacy, and trust levels of distributed systems and the Internet of Things, we concentrate on two areas of the design phase in this thesis. First, we focus on the context of Internet of Things systems and examine the early design stage, during which a system's architecture is being built. Second, we look at the late design stage, which is when models specifically, executable models and prototypes are created with an emphasis on Internet of Things systems the broader context of distributed systems. We confine our effort to the active object paradigm for the modeling associated with the late design phase. Specifically, we find methods for leveraging a security and privacy functionality framework to raise the overall security level of IoT systems, a static analysis tool to identify potential flaws that may lead to distributed denial of service (DDoS) assaults. Furthermore, we created a language-based strategy to give smart contracts privacy, safety, security, and confidence.

Keywords: *IOT, Gigbee, HMM and Routing Protocols.*

1. INTRODUCTION

IoT connected to an Internet network that allows them to collect and exchange data. Internet of Things is now a mature technology that has moved beyond its early stages and on a path to transform our This number will rise to approximately 20 billion in 2020.

Internet of things is a revolution in technology that has many potential applications, such as smart health care, fire detection and environment monitoring. IoT is a web-enabled ecosystem that includes smart devices, processors, sensors and communication hardware. IoT affects almost all aspects of society, improving security through surveillance and monitoring. It also improves quality of life and offers a wide range of services and production without impacting the needs of the human. The connections between machines, objects, and people are increasing exponentially. IoT has grown worldwide. From 2019 to 2023, the expenditures on hardware and software for IoT-related projects will increase from US$726 to US$1.1 trillion [3]. IoT connects various heterogeneous devices like sensors, actuator, RFID etc. The sensor nodes used in large quantities to cover the entire sensing area. They have limitations such as a limited communication range, low battery power and lower processing power. Sensors are primarily used to sense and transmit data to the destination. These sensor nodes have limitations that limit the range of

data transmission. To transmit data to the basestation (BS) in the network, the nodes must work together. In precision farming for example, sensors can be deployed over a large area in order to gather soil data. To measure real-time weather conditions like rainfall and humidity in climate measurement sensors are placed on fields. If any weather disturbance is detected, an alert will be sent [5]. Some examples like military surveillance, the sensors can be positioned randomly while for some applications they are fixed in position. According to the application, sensors can be deployed deterministically or randomly. IoT operations also require different topologies [7]. IoT also creates bonds between the industry and the society and activates various connections between humans and machines. Next, we will discuss the IoT Architecture and its Components.

IoT touches almost every area, a lot of applications based on the IoT technologies coming over time. Different type of application needed different type (topology), coverage, size of the network applications of IoT can be categories in 4 types: multimedia oriented, person oriented, system oriented, and scalar content related applications. Application like smart home, smart surveillance, assisted driving, patient health real time monitoring etc. are some of the applications comes in multimedia content. Smart parking system, automatic update in information of social networks etc. are comes under person oriented applications. System oriented applications includes monitoring critical environmental parameters etc. Lastly, applications related to the scalar content are inventory management, tracking, monitoring of energy consumption etc [8-11]. Section 1 defines the introduction, section 2 works on literature survey, section 3 with methodology section 4 defines results and finally conclusion

2. Background Work

IoT is affecting almost every aspect of life, and as IoT technology advance, so are the applications built upon them. Various applications need varying network topologies, coverage, and sizes. Four categories may be used to group IoT applications: multimedia-focused, person-focused, system-focused, and scalar content-related apps [11]. Applications that come with multimedia material include those for smart homes, smart surveillance, assisted driving, real-time patient health monitoring, and more. Person-oriented applications include things like smart parking systems and social network information updates that happen automatically. Applications that are system-oriented include keeping an eye on important environmental elements. Finally, scalar content applications include tracking, inventory management, energy usage monitoring, etc.

Smart Grid: In order to collect and analyse data from transmission lines, substations, data distribution centres, and customers, smart grid functions as a data transmission network that is connected to the power grid [12]. The smart grid provides distributors and consumers with analytical information for power regulation based on the data collected. WSN, wired, public, or private networks may be utilised for communication in a smart grid design. Because smart grids are susceptible to cyberattacks, the architecture of smart grids should ensure data integrity, availability, and confidentiality. The perception layer, network layer, cloud management layer, and applications layer make up the four layers of the smart grid's design [13].

Smart Industries: The Internet of Things (IoT) industries, organisations, and intelligent processes by providing a solid technical foundation. Some of the likely needs of the current industrial situation include cost reduction, revenue growth, quality control, security, and safety. The employee collection, sometimes referred to as the industrial Internet of things, uses smart devices linked to an active internet to do work related to company [14]. Industrial Internet of Things (IIoT) lowers the overhead of data management for active users linked to the internet and oversees the crowdsourcing process. Crowdsourcing also assists in solving millions of users' online issues in order to get data and feedback for projects [15]. From this point forward, the cloud server's computational burden and storage expenses are reduced by outsourcing crowdsourced IIoT data. Crowdsource data outsourcing raises the possibility of malevolent actors and computational overhead.

Smart Cities: IBM created the idea of a "smart city" by using the Internet of Things' sensing and communication capabilities. The many demands of humans, such as daily sustenance, public safety, municipal services, commercial services, environmental protection, and so on, are met by smart cities [16]. Three layers make up the architecture of a smart city: the network layer, the application layer, and the perception layer [17]. Smart parking, smart street lighting, smart surveillance, water and waste management are all part of the smart city.

3. Methodology

In IoT, the traditional networking devices such as routers and switches are replaced with generic data forwarding devices known as IoT switches. Switches forward the data packets as per the network control rules, known as row-rules, dictated from the control plane device, known as IoT controller. A network row is defined as a sequence of packets sharing specific attributes of interest. For example, all data packets destined to node can be considered as a row if there exists a requirement to control the trafic toward node v. Controller and switches communicate through a control channel (depicted as dotted lines using a south-bound interface, the most popular being the OpenFlow protocol [11]. The control channel can be a separate dedicated network, known as out-of-band control, or can share the same network infrastructure of the data plane, known as in-band control. The controller is assumed to have the global network view which is used to compute the flow-rules. The flow-rules are further sent to the switches for handling packets corresponding to each flow. Each switch is integrated with flow tables to store the required flow-rules.
A flow-rule within a flow-table is composed of three parts: (i) match-fields, (ii) actions, and (iii) flow-rule attributes.
1. Match-fields: The attributes of a packet corresponding to each layer, specifically Layers 2–4 of the TCP/IP protocol stack, along with the ingress port constitute the match-fields. Examples of match-fields include source and destination IP addresses, source and destination Medium Access Control (MAC) addresses, and the source and destination ports of the transport layer protocols. OpenFlow v1.0 [12] defines 12 match-fields while OpenFlow v1.5 [13] improves the granularity to 45 attributes.
2. Actions: The actions that need to be taken on the packets which have matched with a flow-rule are specified in the Action field. Examples of actions include OUTPUT (to the specified port), DROP, CONTROLLER, the modification of packet attributes. In this thesis, we introduce a new action STORE for the controlled buffering of packets in IoT switches, thereby, handling link disruptions in software defined wireless networks.
3. Flow-rule attributes: Different counters associated with a flow-rule constitute the flow-rule attributes. Examples include idle-timeout, hard-timeout, rule priority, and the number of rule-hits. Idle-timeout defines the lifetime of a flow-rule without a rule-hit, i.e., the rule gets removed from the flow-table if no packets matches the rule within the time unit specified as idle-timeout. On the other hand, hard-timeout removes the flow-rule after the specified time units irrespective of a flow-rule hit or miss. The flow-rule attributes are sent to the controller on request for generating the global network view.

In earlier computing, authentication was the responsibility of the central server. When a machine wants to communicate with another machine, it requests the central server and then the central server starts the process of MA between the two. The three way authentication, Diffie-Hellman, was also popular. Although both the algorithms work very well, these protocols are not suitable to be included into an IoT environment. Because of the fact that the devices under an IoT environment are highly resource constrained, new lightweight and energy efficient protocols for MA are needed [17]. The lightweight MA protocol works on two basic principles. First, the authentication process should be handled only by the communicating devices, i.e. without any involvement of the central server. Second, the security, storage, area, and battery requirement should be as per the requirement of resource constrained devices. Many works have been already proposed in this domain. Different researchers include different methods in computing the secret value to be used in the process of MA. One of them is Kulseng. Kulseng uses the concept of PUF (Physical Unclonable Function) in his design. Scholar presents a similar lightweight and energy efficient MA protocol. The proposed protocol, named DeeR-MA, is based on Hashing and PUF. It reduces the number of computations at both ends and also provides a high level of security within the requirements of a constrained environment.

Secure zigbee configuration for iot systems

In our simulations of attacks on a ZigBee Network, we have found that only protecting the device configurations was not enough to secure the ZigBee. The removal of a ZigBee node is not detected and the new key generated and sent to other devices in the network by the coordinator. It is important to detect the absence of nodes in a network to stop stolen ZigBee devices from being re-used to join and compromise a network. We have created a “heartbeat” between the coordinator, and router to solve the problem. It is a message that the sender transmits every 200ms in order to inform the receiver of its existence. If the recipient does not get notified non-existence of that sender in the network. This will help prevent future attacks on the network.
We have encrypted the entire data transmitted by the ZigBee device at the application layer. The AESLib.h is used to encrypt and decrypt data such as sensor data, "heartbeat" data or data about the state of the device. AESLib.h uses a 128-bit or 256 bit encryption key. Our system is more secure with the encryption of the application and network layers. This reduces the chance and ability for an attacker to

be able to decrypt data from our IoT Framework in real-time. By connecting the coordinator to the computer serially, the encrypted data can be decrypted. The coordinator configures the Ethernet shield's MAC and IP addresses. A LED is connected to the coordinator, which acts as a light. It turns on or off based on data sent from the router. The coordinator decrypts any data received from the router using the key used in the router. It then validates the information and takes the appropriate action.

4. Results and Discussion

The DDoS attack is comprised of energy fatigue, flooding and resource depletion attacks. The energy exhaustion attack is classified as an DDoS assault in the research. The ZigBee WSN's E-IDSEP that consists of a more efficient watchdog system an Hidden Markov Model, is designed to recognize this attack (HMM). The improved watchdog system is used to keep an eye on node activity. The Hidden Markov Model is used to forecast the energy dissipation rate of sensor nodes [19]. (HMM). The monitored nodes' leftover energy are collected by the watchdog nodes. Additionally, it calculates the reported residual energies' actual energy consumption estimates and contrasts them with HMM's anticipated energy consumption values. The EE-IDSEP approach is used to identify DDoS assaults on nodes with abnormally high energy consumption. The suggested system's functional flow diagram, incorporates topology discovery by sink, optimal watchdog deployment, and DDoS assault detection.
Utilizing HMM, estimate the energy dissipation rate of distinct states
ECollected residual: Energy that was still present at the nodes that were being watched.
Calculated residual: Watchdog node's estimated residual energy based on used and initial energy.

Algorithm:
Step 1: The watchdog node uses an HMM filter to estimate the energy (E) that has been spent.
Step 2: The watchdog node combines all the energy from all monitored nodes.
Step 3. Watchdog determines what is left ECalculated (difference from the energy initial and E consumed)
Step 4: Energy consumption is normal if E Collected Residual > E Calculated Residual.
Step 5: If the energy consumption is abnormal if the E Collected residual is more than the E Calculated residual.
Step 6: If energy is anomalous, the network connection of the attacker node will be severed; otherwise, move to step 1.
Table 1:Parameters

NoofNodes	15, 45, 85, 115
Area	110 X 110 m2
RoutingProtocol	AODV,STR,OSTR
SimulationTime	100sec
TrafficSource	Poisson
Attackers(DDoS&Wormholeattack)	10&20no’s
NodeEnergy	1Joule
Propagation	TwoRayGround
Antenna	Omnidirectionalantenna
MAC	IEEE 802.15.4

By using NS2 simulator, the planned and current IDS [12] are simulated. The table-1 displays the parameters that were utilised for this simulation. The network comprises of 100 nodes spread out randomly over a 110 × 110 m2 geographical region. The DDoS attacker nodes and wormhole attacker node pair are dispersed at random across the network. In order to alter the number of holes, DDoS assaults, and node density, effectiveness of the suggested strategy is measured in terms of the ratio of packet

delivery The energy used, average end-to-end latency, false positive and detection rates, and average detection time are also included.

EE-IDS proposed for wormhole detection This section provides examples of the simulation outcomes for the present EE-TSW and the planned EE-IDS [12]. The simulation results provided indicate the average end-to-end latency, energy consumption, and packet delivery ratio in relation to the number of wormhole assaults. the proposed and current systems' average detection times, false positive rates, and detection rates overall.

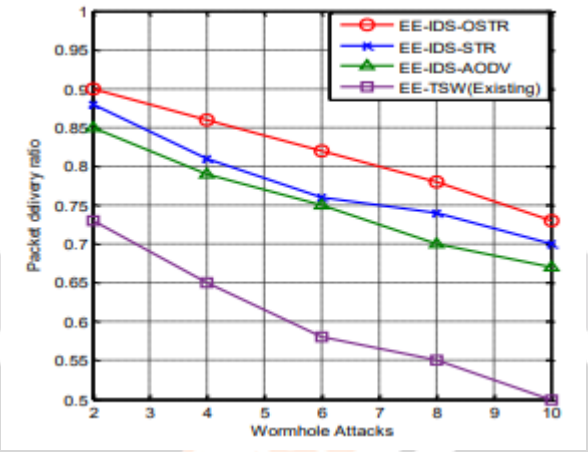

Figure1: Ratio of delivery for packages vs. Attacks

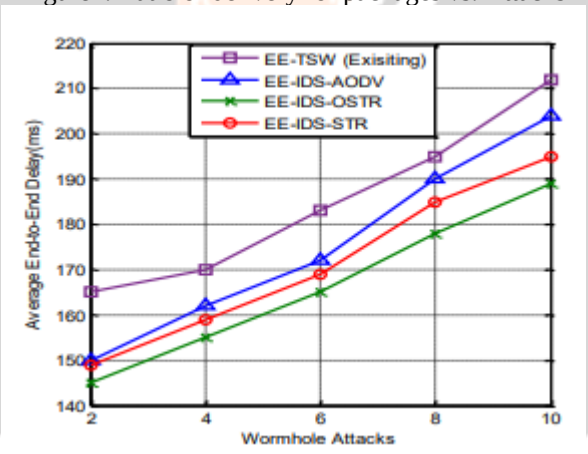

Figure 2: Avg. End-to-End Delay Versus Attacks

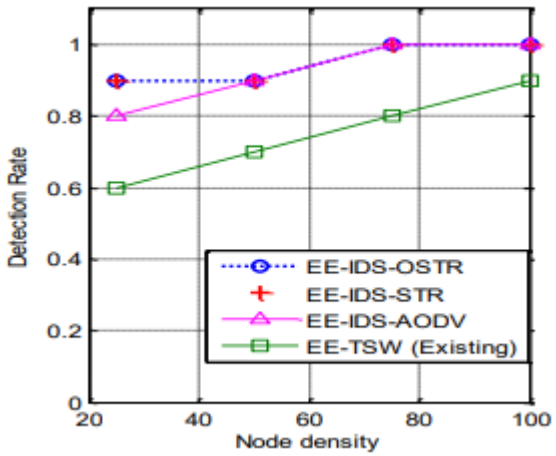

Figure 3: Node density and Detection rate

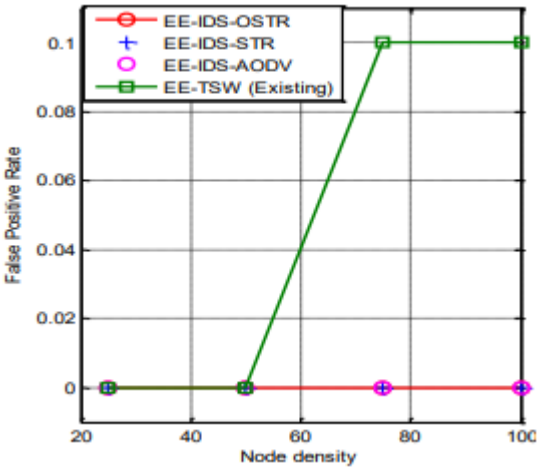

Figure 4: False Node density and Positive rate

This section displays the simulation outcomes for the present EE-TS system and the planned EE-IDSEP[12]. The simulation results displayed demonstrate the average end-to-end latency, energy consumption, and packet delivery ratio relative to the number of DDoS assaults. the proposed and current systems' average detection times, false positive rates, and detection rates overall. According to the simulation findings, the proposed EE-IDSEP performs better than the EETS in the event of DDoS assaults by around 10% in terms of transmission ratios, 10% in terms of end-to-end latency, and 15% in terms of energy usage. It has been shown that the EE-IDSEP system is more efficient than the EETS system in terms of performance parameters like detection time, False Positive Rate (FPR), and detection rate.

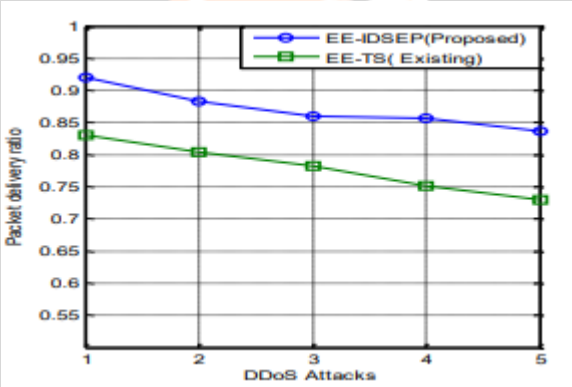

Figure 5:Attacks and Packet delivery ratio

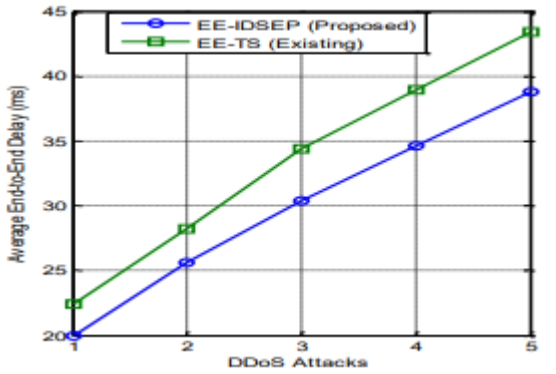

Figure 6: Avg. Attacks and End-to-End Delay

5. CONCLUSIONS

To detect threats from wormholes and DDoS attacks on ZigBee-based wireless sensors, two protocols called EEIDS and EE-IDSEP protocols are recommended in this study. Simulation results show that the EEIDS that uses the STR and OSTR protocol performs better in comparison to the EETSW by around 28 33% and 3 percent in terms of the transmission ratio, 8.8% and 6.6 percent for end-to-end latency 10.5 percent and 12.3 percentage for energy consumption for attacks via wormholes. Similar to the way

that suggested EEIDSEP beats EETS when it comes to DDoS assaults, it can do this by around 10% more efficient packet delivery, a 15% reduction in end-to-end time, and a 10% improvement in energy usage. Key IDS performance indicators, such as detection rate, false positive rate, and average detection times, have also shown that the proposed IDS performs better than the current IDS. Accordingly, it can be said that a range of ZigBee applications that need safe security but don't consume a lot of energy may employ the EEIDS and EE-IDSEP. Another way to further this research is to use a ZigBee WSN mobility model to detect DDoS assaults and wormholes.

Every layer of the IoT architecture is open to assaults. As a result, there are several security dangers and demands that must be met. The current status of IoT research is mostly focused on access control and authentication protocols, however due to the fast advancement of technology, it is crucial to combine new networking protocols like IPv6 and 5G to accomplish the progressive fusion of IoT topologies. The primary objective of this chapter was to bring to light important security issues related to IoT. It focused on threats to security and how to defend against them. A lack of security measures makes many IoT devices easy targets. Even these can be infected by hackers without their victims' knowledge. This chapter covers the security requirements, including confidentiality, integrity and authentication. This study addresses several IOT applications. This article, which highlights the main problems in IoT Security and fosters a better understanding of risks, their characteristics, and the invasion of different entities, like businesses and intelligence agencies will hopefully be useful to security researchers. In this article, we have discussed the basics of Internet of Things (IoT), the applications it has and the risks that are associated with them. Security concerns are increasing exponentially as the number of Internet of Things devices grows. As the Internet of Things (IoT), which is increasingly popular, becomes a target for cyber attacks, security has become a more difficult task. When the Internet of Things integrates with other platforms and cloud computing, it is a concern. So, we have identified a variety of cyber security risks that Internet of Things (IoT) applications face in this article and have also attempted to provide mitigation strategies to make IoT a more reliable and safe system. We included many effective and simple responses for these types of cyber security threats. This should aid in further research into the security issues and give more thorough solutions.

REFERENCE

1) M. Abomhara and G. M. Koien, "Security and privacy in the Internet of Things: Current status and open issues," in Int'l Conference on Privacy and Security in Mobile Systems (PRISMS), 1-8, 2014.
2) K. Zhao and L. Ge, "A survey on the internet of things security," in Int'l Conf. on Computational Intelligence and Security (CIS), 663-667, 2013.
3) L. Atzori, A. Iera, G. Morabito, and M. Nitti, "The social internet of things (siot)–when social networks meet the internet of things: Concept, architecture and network characterization," Computer Networks, vol. 56, 3594-3608, 2012.
4) M. Leo, F. Battisti, M. Carli, and A. Neri, "A federated architecture approach for Internet of Things security," in Euro Med Telco Conference (EMTC), 1-5, 2014.
5) P. N. Mahalle, B. Anggorojati, N. R. Prasad, and R. Prasad, "Identity authentication and capability based access control (iacac) for the internet of things," J. of Cyber Security and Mobility, vol. 1, 309-348, 2013.
6) M. Farooq, M. Waseem, A. Khairi, and S. Mazhar, "A Critical Analysis on the Security Concerns of Internet of Things (IoT)," Perception, vol. 111, 2015.
7) R. Roman, P. Najera, and J. Lopez, "Securing the internet of things," Computer, vol. 44, 51-58, 2011.
8) R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things,"Computer Networks, vol. 57, 2266-2279, 2013.
9) Prasadu Peddi, & Akash Saxena. (2014) “Exploring The Impact Of Data Mining And Machine Learning On Student Performance”, ISSN-2349-5162, Vol 1, Issue 6, pp:314-318.
10) https://irdeto.com/news/new-2019-global-surveyiot-focused-cyberattacks-are-the-new-normal/
11) J. M. Kizza, Guide to Computer Network Security.Springer, 2013.
12) L. Atzori, A. Iera, G. Morabito, The Internet of Things: A survey, Comput Netw. 54 (2010) 2787–2805.
13) Prasadu Peddi, & Dr. Akash Saxena. (2016). STUDYING DATA MINING TOOLS AND TECHNIQUES FOR PREDICTING STUDENT PERFORMANCE. International Journal Of Advance Research And Innovative Ideas In Education, 2(2), 1959-1967.
14) A.P. Castellani, N. Bui, P. Casari, M. Rossi, Z. Shelby, M. Zorzi, Architecture and protocols for the Internet of Things: A case study, in: 2010: pp. 678–683.
15) M. Yun, B. Yuxin, Research on the architecture and key technology of Internet of Things (IoT) applied on smart grid, Advances in Energy Engineering (ICAEE). (2010) 69–72.

16) https://www.educba.com/applications-of-iot/
17) https://towardsdatascience.com/top-14-iot-trendsto-expect-in-2020
18) Pushpa Latha Thumma, Prasadu Peddi (2021), "Survey Of Iot Threats And Countermeasures: Identifying Solutions And Addressing Future Challenges", ISSN: 1735-188X, Volume 18, Number 6, pp:7977-7982.