Journal Homepage: -www.journalijar.com
INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)
ISSN NO. 2320-5407

Article DOI:10.21474/IJAR01/7183
DOI URL: http://dx.doi.org/10.21474/IJAR01/7183

RESEARCH ARTICLE

A SURVEY OF INTRUSION DETECTION SYSTEM IN IOT DEVICES.

S. Suganthi and Dr. D.Usha.
Research Scholar, Asst. Professor, Department of Computer Science, Mother Teresa Women's University, Kodaikanal.

……………………………………………………………………………………………….....

Manuscript Info

……………………….
Manuscript History

Received: 02 April 2018
Final Accepted: 04 May 2018
Published: June 2018

Keywords:-
Intrusion Detection System, Internet of Things, Cyber security.

Abstract

………………………………………………………………
Now in this era of science and technology, the computer may take a vital role to store and disseminate knowledge to the public. Through the internet technology, the people can get the information from any corner of the world by anyone and also distributing the information is easier. The internet has made our life become easier and more convenient but also has its dark side too. The biggest nuisance and threat for the internet community of the world has to be the hacker and spammers in the signs of intruders. Specifically the threats are created everyday by individuals and organizations which may attack or misuse the computer system. To find out the intruder and intrusion is an open issue because of the complexity of computer infrastructure. Internet of Things (IoT) is a new paradigm that connects the internet and physical objects in different domains such as home automation, industrial process, human health and environmental monitoring. . To handle the intrusion detection in IoT is not an easy task due to the IoT device specification, standards and protocol stacks. . However, there are lots of key issues addressing security concerns of IoT and need more research effort to be solved. This paper gives a complete survey about the taxonomy, summarized and organized recent research results of Intrusion detection system in IoT. Through this study the researchers are easy to detect the security loopholes arising out of the information exchange technologies in Internet of Things and also learn the various security attacks and approaches to mitigate those attacks.

……………………………………………………………………………………………….....

Introduction:-

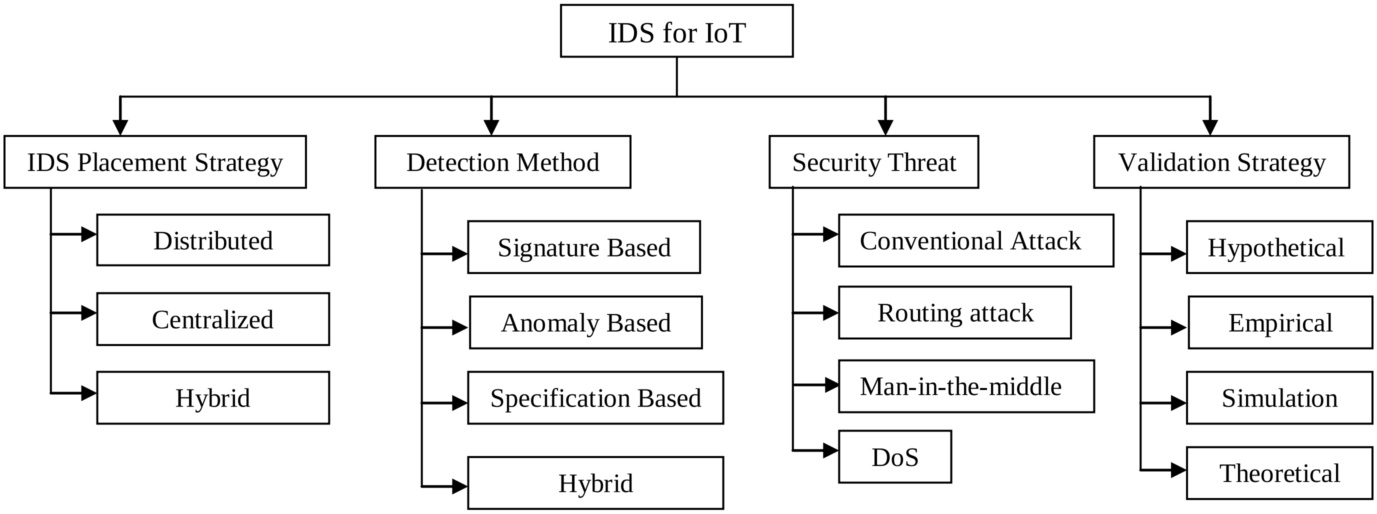
Intrusion detection is a software or hardware which can detect the unauthorized user actions of computer system. IDSs can be classified as Network-based IDS (NIDS) and Host-based IDS (HIDS). Network-based IDS (NIDS) connects to one or more network segments and monitors network traffic for malicious activities. Host-based IDS (HIDS) is attached to a computer device and monitors malicious activities occurring within the system. The IDS works as an alarm or network observer it avoids damage of the systems by generating an alert before the attackers begin to attack. It can detect both internal and external attacks. Internal attacks are launched by malicious or compromised nodes that belong to the network whereas external attacks are launched by third parties who are initiated by outside network. IDS detect the network packets and determine whether they are intruders or legitimate users. The main components of IDS are Monitoring, Analysis and detection. The monitoring module monitors the

Corresponding Author:- S.Suganthi
Address:-Research Scholar, Department of Computer Science, Mother Teresa Women's University, Kodaikanal.

network traffics, patterns and resources. Analysis and Detection is a core component of IDS which detects the intrusions according to specified algorithm. Alarm module raised an alarm if intrusion is detected.

IoT is an emerging technology that has attracted a considerable number of researchers from all around the world. There have been major contributions making this technology adapted into our daily life. It covers many fields including healthcare, automobiles, entertainments, industrial appliances, sports, homes, etc. The pervasiveness of IoT eases some everyday activities, enriches the way people interact with the environment and surroundings, and augments our social interactions with other people and objects. In this paper present a complete catalog of IDS for IoT, security breach of IoT were reviewed substantially. Requirements and challenges of security measures in IoT were analyzed and collected under different headings.

Taxonomy Of Ids For Iot:-



Ids Placement Strategy:-

Distributed Ids Placement Strategy:-

In a distributed IDS placement, the IDS placed every physical object. Oh et al. [1] proposed distributed lightweight IDS for detecting attacks. They suggested two techniques such as auxiliary shifting and early decision. The main goal of this IDS to decrease the number of matches needed for detecting attacks. The results are compared with Wu-Manber algorithm. Lee et. al.[2] also proposed a lightweight IDs which monitor the node energy consumption for detecting intrusions. The main objective of this IDs to minimize the computational resources needed for intrusion detection. This IDs also manage the node energy and control the inbound and outbound traffic. If the IDS detect any attacks it broadcasts a message to alert all nodes.

Centralized Ids Placement Strategy:-

In a centralized IDS placement, the IDS placed in a centralized component. Cho et al. [3] proposed a solution for analyzing the packets that pass through the border router between the physical and the network domain. This work is monitoring only the border router traffic. Kasinathan et al. [4] also employed the centralized placement, but they took into consideration the IDS protection against a DoS (Denial of Service) attack. This way, the authors decided to deploy the IDS analysis engine and the IDS reporting system in a powerful dedicated host. They deployed the IDS sensors in the Low power and Lossy Networks (LLN), which were responsible for sniffing the network traffic and sending this data to the IDS analysis engine. The IDS dedicated host is wire connected to the IDS sensors, avoiding the transmission of IDS data and network regular data in the same wireless network. Therefore, if a DoS attack degrades the wireless transmission quality, IDS data transmission would not be affected.

Hybrid Ids Placement:-

Hybrid IDS placement combines the concepts of centralized and distributed placement to take advantage of their strong points and avoid their drawbacks. The first approach for hybrid placement organizes the network into clusters or regions, and only the main node of each cluster hosts an IDS instance. Then, this node becomes responsible for monitoring the other nodes of its cluster. The hybrid placement IDSs may be designed to consume more resources than distributed placement IDSs. Amaral et al. [5] proposed an IDS for IoT using this approach. In this work, selected nodes in the network host an IDS. These selected nodes (watchdogs) aim to identify intrusions by eavesdropping the exchanged packets in their neighborhood. The watchdog decides whether a node is compromised according to a set of rules. Each watchdog has a particular set of rules because each component in the network might have a different behavior. For example, a border router usually experiences higher rates of messages than a regular node. The advantage of this approach relies on allowing the construction of a different set of rules for each area of the network.

Types Of Ids:-

Signature Based Ids:-

In signature-based approaches, IDSs detect attacks when system or network behavior matches an attack signature stored in the IDS internal databases. If any system or network activity matches with stored patterns/signatures, then an alert will be triggered. In [6], Liu et al. proposed a signature-based IDS that employs Artificial Immune System mechanisms. Detectors with attack signatures were modeled as immune cells that can classify datagrams as malicious (non-self element) or normal (self-element). Moreover, detectors can evolve to adapt to new conditions in the monitored environment.

Anomaly Based Ids:-

This technique is also known as event-based detection. This technique identifies malicious activities by analyzing the event. Firstly, it defines the normal behavior of the network. Then, if any activity differs from normal behavior then its mark as an intrusion. In this approach, a malicious node can be detected by matching the current protocol specification with previously defined protocol state. This approach detects attacks more efficiently than Signature based IDS. Thanigaivelan et al. [7] briefly introduced a distributed internal anomaly detection system for IoT. The principle of the proposed IDS is to look for any discrepancies in the network by monitoring the characteristics of one-hop neighbor nodes such as packet size and data rate. According to the authors, the system learns and derives the normal behaviors from the monitored information.

Specification Based Ids:-

This technique is somewhat similar to anomaly detection technique. In this technique, the normal behaviour of the network is defined by manually, so it gives less incorrect positives rate. This technique attempts to excerpt best between signature-based and anomaly based detection approaches by trying to clarify deviations from normal behavioral patterns that are created neither by the training data nor by the machine learning method. The development of attack or protocol specification is done by manually so it takes more time. So, this can be a disadvantage of this approach. Amaral et al. [8] proposed a specification-based IDS that allows the network administrator to create rules for attack detection. When one of these rules is violated, the IDS sends an alert to the Event Management System (EMS). The EMS runs on a node without resource constraints to correlate the alerts for different nodes in the network.

Hybrid Approaches:-

Hybrid approaches use concepts of signature-based, specification-based and anomaly based detection to maximize their advantages and minimize the impact of their drawbacks. Krimmling and Peter[9] tested anomaly and signature-based IDSs using the IDS evaluation framework that they proposed. The results showed that each approach failed in detecting some kinds of attacks. According to the authors, a combination of these approaches could address a wider range of attacks with single IDS.

Security Threats:-

The objective of this subsection is to discuss how different attack types have been addressed in the IDS proposals for IoT. Enabling IoT solutions involves a composition of several technologies, services, and standards, each one with its security and privacy requirements. With this in mind, it is reasonable to assume that the IoT paradigm has at least the same security issues as mobile communication networks (e.g., WSNs), cloud services and the Internet.

Summerville et al. [10] focused on conventional attacks. Summerville et al. assessed the performance of their IDS with conventional attack scenarios that included worm propagation, tunneling, SQL code injection, and directory traversal attacks.

Cyber-Attacks On Iot Applications:-

Sinkhole Attack:-

In this attack, malicious node at- tracts network traffic towards it. To launch these types of attack, a malicious node attract all adjacent nodes to forward their packets through the malicious node by showing its routing cost minimum. The attacker creates an attack by introducing false node inside a network .R.Stephen et al.[11] proposed an Intrusion Detection System (IDS) to detect the sinkhole attack in the network which uses the RPL as a routing protocol. The proposed algorithm uses the detection metrics such as number of packets received and transmitted to validate the Intrusion Ratio (IR) by the IDS agent. A technique is proposed to identify whether the router node is a malicious node or not using the IR value. If IDS system detects the malicious node, it sends the alert message to the leaf nodes to isolate the malicious node in next data transmission. The aim of the proposed work is to minimize the Intrusion Ratio.

Wormhole attack:-

In this attack, the adversary node creates a virtual tunnel between two ends. An adversary node acts as a forwarding node between two actual nodes. The wormhole attack can also be used to convince two distinct nodes that they are the neighbors by relaying packets between two of them. Pavan Pongle Gurunath Chavan[12] proposed system is a novel intrusion detection system for the IoT, which is capable of detecting Wormhole attack and attacker. The proposed methods uses the location information of node and neighbor information to identify the Wormhole attack and received signal strength to identify attacker nodes. Design of such system will help in securing the IoT network and may prevents such attacks. This method is very energy efficient and only takes fixed number of UDP packets for attack detection, hence it is beneficial for resource constrained environment.

Selective Forwarding Attack:-

In this attack, malicious node acts as a normal node but it selectively drops some packets. Black hole attack is the simplest form of selective forwarding attack in which all packets are dropped by the malicious node. Shapla Khanam et.al [13] we propose a game - theory based attack model to analyze the malicious behavior of attackers in the IoT networks. In this model two players are involved in the game where player_1 and player_2 play to maximize and minimize the throughputs of the network respectively. Additionally, a hop-by-hop acknowledgement (ACK) algorithm is also presented detect malicious attacker in order to defend networks from selective forwarding attacks in IoT.

Sybil Attack:-

In this attack, the node has multiple identities. The routing protocol, detection algorithm and co-operation processes can be attacked by a malicious node . Kuan Zhang[14] et.al defines three types Sybil attacks: SA-1, SA-2, and SA-3 according to the Sybil attacker’s capabilities and then present some Sybil defense schemes, including social graph-based Sybil detection (SGSD), behavior classification-based Sybil detection (BCSD), and mobile Sybil detection with the comprehensive comparisons. Finally, they discuss the challenging research issues and future directions for Sybil defense in IoT.

Denial Of Service (Dos) Attack:-

This attack can damage the availability of resources. When this attack is made, resources are not available to legitimate users. Such type of attacks, when launched by various malicious nodes is called DDoS. This attack may affect the network resources, bandwidth, CPU time etc. Tasnuva Mahjabin et. Al [15] present a comprehensive survey of distributed denial-of-service attack, prevention, and mitigation techniques. They provide a systematic analysis of this type of attacks including motivations and evolution, analysis of different attacks so far, protection techniques and mitigation techniques, and possible limitations and challenges of existing research. Finally, some important research directions are outlined which require more attentions in near future to ensure successful defense against distributed denial-of-service attacks.

Validation Strategy:-

According to D.Chrun[16] presents a validation consists of checking that the built model behaves with satisfactory accuracy within the study objectives. There are many validation techniques, and they may be distinguished by two sources of information: experts and data. While the use of experts provides a subjective and often qualitative model validation, the use of data may allow a quantitative and more objective validation. Our goal here is to investigate the validation strategy employed in the intrusion detection methods for IoT.

Hypothetical:-Hypothetical examples, having unclear relation to actual phenomena and degree of realism.

Empirical:-Empirical methods, such as systematic experimental gathering of data from operational settings.

Simulation:-Simulation methods of some IoT scenario.

Theoretical:-Formal or precise theoretical arguments to support results.

Security Issues In Iot Architecture:-

The biggest challenge of IoT is ensuring data and privacy protection. The key technologies of IoT are RFID technology, sensor technology, embedded system technology and nanotechnology; therefore, one of the main risks comes from the technology of construction. Since IoT is the integration of multiple heterogeneous networks it is difficult to achieve a reliable connection between the individual nodes in IoT due to the nodes constantly changing. IoT architecture can be divided into three layers: sensing layer, transportation layer and application layer (Table I).

Application layer	Transport layer	Sensing layer
Information availability, user authentication, information privacy, data integrity, IoT platform stability, middleware security, management platform	DOS/DDOS attacks, forgery/middle attack, heterogeneous network attacks, WLAN application Conflicts, capacity and connectivity issues etc.	Interruption, interception, modification, fabrication, uniform coding for RFID, conflict collision for RFID etc.

Attack Mitigation Techniques:-

Tasnuva Mahjabin et.al[17] present a comprehensive survey of distributed denial-of-service attack, prevention, and mitigation techniques. We provide a systematic analysis of this type of attacks including motivations and evolution, analysis of different attacks so far, protection techniques and mitigation techniques, and possible limitations and challenges of existing research. Finally, some important research directions are outlined which require more attentions in near future to ensure successful defense against distributed denial-of-service attacks.

RaviTeja Gaddam and Dr. M. Nandhini [18] tries to analyze several attacks that are targeting the IoT network and discusses the recent works to provide security for IoT. They also propose an architecture for efficient IDS in IoT network. propose a novel Intrusion Detection System to thwart the attackers and to protect the IoT connected devices from a variety of attacks. Authors designed and successfully evaluated the enhanced Snort IDS in conventional networks.

V.Gayathri et.al [19] proposed a system incorporates security along with automation using IOT. The security module successfully sends alerts upon detecting intruder using wireless sensors and biometric techniques where owner further can take necessary actions also owner can successfully automate environment through app thus enabling owner to simplify complex tasks, enhance convenience and comfort, save energy efficiently, access and use home systems anywhere and enjoy completely security.

Aastha Puri1, Nidhi Sharma [20] proposed several machine learning and other suitable approaches proposed to solve the problem of intrusion have been reviewed and conclusion on the basis of the performance parameters is drawn. Many approaches have been used in the security analysis of the computer networks. In one approach Particle Swarm Optimization algorithm is used with the unsupervised classification algorithm. The IDCPSO technique shows higher speed of convergence and high detection rate as compared to the genetic approach. In another method PSO algorithm is used with the Map Reduce approach which improves the parallelization in the approach of data mining. The detection in large amount of data is improved and the speed of operation is improved as compared to the basic approach. Some use unsupervised clustering using the grid based and density based approaches. This helps improving the anomaly detection rate of the process. In future several other machine algorithms must be implemented with unsupervised clustering approaches.

Summary Of Intrusion Detection System For Iot Devices:-

Ref	Objective	Methodology	Achievements
[1]	To detect attacks	auxiliary shifting method and the early decision scheme	speedup of up to 2.14 compared to the traditional pattern-matching algorithm
[2]	To implement a secure communication in Internet of Things	The 6LoWPAN energy consumption models for mesh-under and route-over routing schemes also concerned.	The sensor nodes with irregular energy consumptions are identified as malicious attackers.
[3]	To detect threat in Botnet.	A novel mechanism of Botnet on 6LoWPAN.	analyze the threat of Bot- net on 6LoWPAN and propose a

			mechanism to detect Botnet on 6LoWPAN.
[4]	To detect DoS attacks based on 6LoWPAN	To use DoS detection architecture	It overcomes the resource constraint problems and provides more power to detect complicated attacks.
[5]	Identify intrusion in network-based intrusion detection system (IDS) for IPv6-enabled wireless sensor networks.	The watchdog decides whether a node is compromised according to a set of rules. Each watchdog has a particular set of rules because each component in the network might have a different behavior.	The proposed IDS is used to detect security attacks based on traffic signatures and abnormal behaviors.
[6]	To detect the security threat in the Internet of Things (IoT),	The mechanisms of artificial immune system are applied to the IoT environment	The attack information library is defined. Attacks detected by detectors in the IoT are combined with the attack information library to alarm the manager of the IoT.
[7]	Create an anomaly detection system for Internet-of-things	Monitoring the characteristics of one-hop neighbor nodes such as packet size and data rate. The system learns and derives the normal behaviors from the monitored information.	To detect anomaly in IoT environment.
[8]	Attack detection	The EMS runs on a node without resource constraints to correlate the alerts for different nodes in the network.	Attack detection through EMS
[9]	Tested anomaly and signature-based IDSs	Using IDS evaluation framework	Attack detection successfully.
[10]	To solve conventional attacks	Assessed the performance of their IDS with conventional attack scenarios that included worm propagation, tunneling, SQL code injection, and directory traversal attacks.	Conventional attacks detected
[11]	to detect the sinkhole attack in the network which uses the RPL as a routing protocol.	The proposed algorithm uses the detection metrics such as number of packets received and transmitted to validate the Intrusion Ratio (IR) by the IDS agent. A technique is proposed to identify whether the router node is a malicious node or not using the IR value.	The proposed mechanism calculates the Intrusion Ratio to identify the malicious nodes in the network.
[12]	To detect Wormhole attack and attacker	Designed for resource constrained sensor nodes and able to detect Wormhole attacks of two kind packet relay and encapsulation.	Attack detection rate is high compared with previous methods.
[13]	To analyze and detect selective forwarding attacks to ensure a secure routing.	A game-theory based attack model to analyze the malicious behavior of attackers in the IoT networks.	Detect the malicious attacker in the IoT heterogeneous network
[14]	Survey of Sybil attacks and defense schemes in IoT.	Present various sybil attack detection schemes	Sybil attacks are detected.
[15]	To present a comprehensive survey of distributed denial-of-service attack,	-	Some important research directions are outlined which require more attentions in

	prevention, and mitigation techniques.		near future to ensure successful defense against distributed DoS attacks.
[16]	Tested using validation strategy	Use validation model	Investigate the validation strategy employed in the intrusion detection methods for IoT.
[17]	Survey of DoS attacks and mitigation techniques	-	Important research directions are outlined which require more attentions in near future to ensure successful defense against distributed denial-of-service attacks.
[18]	To analyze several attacks that are targeting the IoT network and discusses the recent works to provide security for IoT.	Proposed a novel Intrusion Detection System to thwart the attackers and to protect the IoT connected devices from a variety of attacks.	Authors designed and successfully evaluated the enhanced Snort IDS in conventional networks.
[19]	Security in IoT	Novel security model is used to secure the IoT environment.	Energy efficient security system in home
[20]	To solve intrusion detection	Particle Swarm Optimization algorithm is used with the unsupervised classification algorithm.	The IDCPSO technique shows higher speed of convergence and high detection rate as compared to the genetic approach

Conclusion:-

In this survey paper mainly focused about IDS research efforts for IoT. Totally 20 papers are selected for the literature which specifically elaborate about the IDS taxonomy, challenges and security attack mitigation approaches. These papers were published between 2014 and 2017. The various attacks are discussed and also present mitigation techniques for handling attacks. This work is used for the researchers those who are working in IDS to get a clear idea about IDS and IoT.

References:-

1. D. Oh, D. Kim, W. W. Ro, A malicious pattern detection engine for embedded security systems in the Internet of Things, Sensors 14 (12) (2014) 24188–24211.
2. T.-H. Lee, C.-H. Wen, L.-H. Chang, H.-S. Chiang, M.-C. Hsieh, A lightweight intrusion detection scheme based on energy consumption analysis in 6LowPAN, in: Y.-M. Huang, H.-C. Chao, D.-J. Deng, J. J. J. H. Park (Eds.), Advanced Technologies, Embedded and Multimedia for Human-centric Computing, Vol. 260 of Lecture Notes in Electrical Engineering, Springer Netherlands, 2014, pp. 1205–1213.
3. E. Cho, J. Kim, C. Hong, Attack model and detection scheme for botnet on 6LoWPAN, in: C. Hong, T. Tonouchi, Y. Ma, C.-S. Chao (Eds.), Management Enabling the Future Internet for Changing Business and New Computing Services, Vol. 5787 of Lecture Notes in Computer Science, Springer Berlin Heidelberg, 2009, pp. 515–518.
4. P. Kasinathan, C. Pastrone, M. Spirito, M. Vinkovits, Denial-of-service detection in 6LoWPAN based Internet of Things, in: Wireless and Mobile Computing, Networking and Communications (WiMob), 2013 IEEE 9th International Conference on, 2013, pp. 600–607.
5. J. Amaral, L. Oliveira, J. Rodrigues, G. Han, L. Shu, Policy and network-based intrusion detection system for IPv6-enabled wireless sensor networks, in: Communications (ICC), 2014 IEEE International Conference on, 2014, pp. 1796–1801.
6. C. Liu, J. Yang, Y. Zhang, R. Chen, J. Zeng, Research on immunity-based intrusion detection technology for the Internet of Things, in: Natural Computation (ICNC), 2011 Seventh International Conference on, Vol. 1, 2011, pp. 212–216.
7. N. K. Thanigaivelan, E. Nigussie, R. K. Kanth, S. Virtanen, J. Isoaho, Distributed internal anomaly detection system for Internet-of-Things, in: 2016 13th IEEE Annual Consumer Communications Networking Conference (CCNC), 2016, pp. 319–320.

8. J. Amaral, L. Oliveira, J. Rodrigues, G. Han, L. Shu, Policy and network-based intrusion detection system for IPv6-enabled wireless sensor networks, in: Communications (ICC), 2014 IEEE International Conference on, 2014, pp. 1796–1801.
9. Krimmling, S. Peter, Integration and evaluation of intrusion detection for CoAP in smart city applications, in: Communications and Network Security (CNS), 2014 IEEE Conference on, 2014, pp. 73–78.
10. D. H. Summerville, K. M. Zach, Y. Chen, Ultra-lightweight deep packet anomaly detection for Internet of Things devices, in: 2015 IEEE 34th International Performance Computing and Communications Conference (IPCCC), IEEE, 2015, pp.1–8.
11. R. Stephen and Dr. L. Arockiam, “Intrusion Detection System to Detect Sinkhole Attack on RPL Protocol in Internet of Things” International Journal of Electrical Electronics & Computer Science Engineering Volume 4, Issue 4(August, 2017) | E-ISSN : 2348-2273.
12. Pavan Pongle and Gurunath Chavan, Real Time Intrusion and Wormhole Attack Detection in Internet of Things. *International Journal of Computer Applications* Volume 121 - Number 9, July 2015.
13. Shapla Khanam, Ismail Ahmedy and Mohd Yamani Idna Idris, An efficient detection of selective forwarding attacks in heterogeneous IoT Networks, FCSIT, 2017: pp 1-8.
14. Kuan zhang et.al, sybil attacks and their defenses In the internet of things, Ieee internet of things journal, vol. 1, no. 5, october 2014.
15. Tasnuva Mahjabin1, Yang Xiao1, Guang Sun2 andWangdong Jiang, A survey of distributed denial-of-service attack, prevention, and mitigation techniques, International Journal of Distributed Sensor Networks, 2017, Vol. 13(12).
16. D. Chrun, Model-Based Support for Information Technology Security Decision Making, Ph.D. thesis, University of Maryland (2011).
17. Tasnuva Mahjabin1, Yang Xiao1, Guang Sun2 andWangdong Jiang, “A survey of distributed denial-of-service attack,prevention, and mitigation techniques” International Journal of Distributed Sensor Networks 2017, Vol. 13(12).
18. Raviteja gaddam1 & dr. M. Nandhini, Analytical approach to enhance the intrusion detection in internet of things network**,**international journal of latest trends in engineering and technology, Vol.(9) issue(3), pp.258-267.
19. V.Gayathri, Malatesh S H, Smart Intrusion Detection System for HomeSecurity, International Journal of Science, Engineering and Technology,2017.
20. Aastha Puri1, Nidhi Sharma, A Survey On Intrusion Detection System, IJEDR | Volume 5, Issue 2 | ISSN: 2321-9939.