DOI: http://dx.doi.org/10.26483/ijarcs.v9i1.5429

ISSN No. 0976-5697

Volume 9, No. 1, January-February 2018

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

INTRUSION DETECTION IN INTERNET OF THINGS (IOT)

Okwori Anthony Okpe
Department of Computer Science
Federal University Wukari,
Wukari, Nigeria.

Odey Adinya John
Department of Computer Science
Federal University Wukari,
Wukari, Nigeria.

Siman Emmanuel
Department of Computer Science
Federal University Wukari,
Wukari, Nigeria.

Abstract: The Internet of Things (IoT) is an ever-growing network of smart objects where one physical object can exchange information with another physical object. Security and privacy of data are one of the prime concerns in today's Internet of Things (IoT). The intrusion detection in internet of things exposes the extent with which the internet of things is vulnerable to attacks and how such attack can be detected to prevent extreme damage. It emphasises on threats, vulnerability, attacks and possible methods of detecting intruders in order to prevent the system from further damage.

Keywords: IOT, security, privacy

1. INTRODUCTION

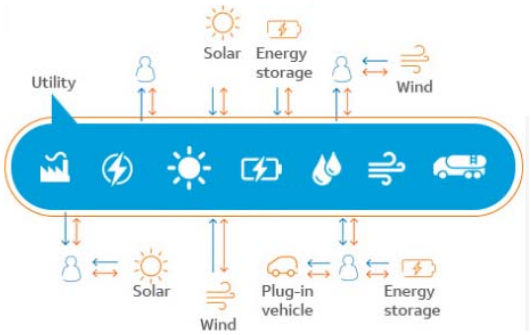
The Internet of Things (IoT) network connects resource-constrained things to the information superhighway (World Wide Web) through the internet protocol version six (IPv6) and internet protocol version six Low-power Wireless Personal Area Network (6LoWPAN).The number of threats and attacks against IoT devices and services are on the increase [1]even when they are secured with encryption and authentication, these things are exposed both to wireless attacks from inside the 6LoWPAN network and from the Internet [2]. Unlike typical wireless sensor networks (WSN), 6LoWPAN networks or IP-connected WSN are directly connected to the untrusted Internet and an attacker can get access to the resource-constrained things from anywhere on the Internet. This global access makes the things vulnerable to intrusions from the Internet in addition to the wireless attacks originating inside 6LoWPAN networks.These vulnerabilities have been showing up targeting the physical interfaces of IoT devices, wireless protocols, and user interfaces [3].Providing security in IoT is challenging as the communication links are lossy, and the devices uses a set of novel IoT technologies such asRouting Protocol for low power and lossynetwork(RPL) [4]. Therefore, the challenge of implementing secure communication in the IoTnetworkcannot be completed without intrusion detection system (IDS)as the IoTcannot be protected against cyber-attacks [5]. A more-realistic approach to develop a security system for IoT comprises of four parts which includes the main prevention component,thedetection component for identifying security breaches,theinvestigation component that determines exactly what happened based on data from the detection component and the post-mortem component that analyzes how to prevent similar intrusions in the future.

Intrusion Detection Systems (IDSs) attempt to identify unauthorized use, misuse, and abuse of computer systems [6]. It can be a software or hardware tools that inspect and investigate machines and user actions, detect signatures of well-known attacks and identify malicious network activity. It aims at observing the networks and nodes, detect various intrusions in the network, and alert the users after intrusions had been detected. It works as an alarm or network observer to avoid damage to the systems by generating an alert before the attackers cause any harm to the system.The IDSs forIoTs monitors several devices connected by a network.

2. COMMON THREATS IN INTERNET OF THINGS NETWORK

As internet users continue to connect more Internet of Things network devices, intruders tend to gain greater surfaces to launch new types of cyber-attacks. This is owned to the fact that, the various devices that now constituted the internet of things network have little security protection against network-borne threats hence very simple to exploit. Intruders can easily exploit poorly protected internet of things network devices to cause varying degree of damages ranging from physical damage, spying, distributed denial of service, among others. Some IoT devices that purses threats to the internet of Things network includes:

- **Smart Grid:**In 2012, the Department of Homeland Security discovered a flaw in hardened grid and router provider RuggedCom's devices. The energy grid of this internet of things device can easily be compromised by attacker when they decrypts the trafficbetween an end user and the RuggedCom device.



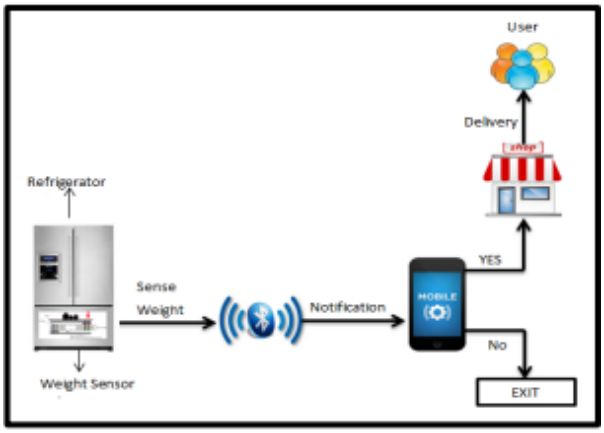
Smart grid [7]

- **Home Network Routers:**Of all the Internet connected devices in homes these days, the network router continues to be by far the most targeted in attacks [8]. "Most Internet routers that are keystone to our home network are riddled with security issues, which make them easy picking for hackers. Most routers worldwide had default or basic username and password combinations, like "admin" and “password” while others have they user address, birthday or name as password. Because of this, most routers are vulnerable to simple password attacks, which is basically an open invitation to malicious hackers.Not surprisingly, attackers have begun taking advantage of vulnerable home routers to create botnets for relaying spam and launching DDoS attacks.

- **Digital Video Recorders (DVRs):** The near ubiquitous set-top boxes, which people use in their homes to record TVs shows, have become another favorite target for attackers. Compromised DVRs have been linked to recent massive DDoS attacks, and researchers have warned of attackers creating large botnets of such devices for use in various malicious ways.As with home routers, DVRs often ship with poor- to nearly nonexistent security controls. Many are connected to the Internet with hard-coded or default passwords and usernames. Often DVRs from multiple manufacturers integrate components from the same supplier. As a result, a security flaw in one product is likely to exist in another vendor's product as well.

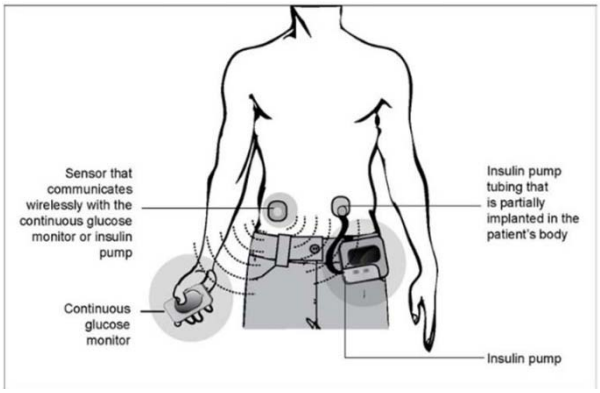
Security vendor Flashpoint recently analyzed malicious code that was used in DDoS attacks involving IoT devices. The company discovered that a large number of DVRs being exploitedby the malware [9] were preloaded with management software from a single vendor. The supplier sold DVR, network video recorder (NVR), and IP camera boards to numerous vendors who then used the parts in their own products. Flashpoint estimated that more than 500,000 network-connected DVRs, NVRs, and IP cameras were vulnerable to the attack code because of a vulnerable component from a single vendor.

Smart refrigerator and other Smart Home Products: AnInternet-connected refrigerator can beused to relay spam. This served as aproof of startling vulnerability of many network-enabled devices being installed in homes these days such as smart refrigerators, televisions, digital assistants, and smart heating and lighting systems.Some smart home products such as refrigerators, personal assistants among others have adequate processing power for botnets attack as well as serving as access points to othernetworks.Thesedevicescould also serve as threats in the enterprise context. For example, a connected refrigerator in a corporate office can provide astartling gateway to other systems that contains corporate data which can be achieved by hacking through the refrigerator to gain network access.Asthe connected refrigerator is on the corporate network that is connected to the enterprise applications, hackers can take advantage of it to gain information on relevant corporate and customer data.



Block diagram of Smart Refrigerator [10]

- **EmbeddedHealthDevices**:Wireless-enabledEmbedded Health Devices such as insulin pumps, pacemakers, and defibrillators are vulnerable targets for cyber-attacks on the internet of things network. Attackers can exploit the unencrypted and commonly weak communications protocols in these devices to remotely control them and manipulate them to behave in potentially harmful ways to the wearers of these medical devices.An attacker could equally take advantage of weaknesses in the wireless management protocol and pairing protocols of devices like insulin pumps to gain remote access to it and get it to release lethal doses of insulin to its wearers.



Continuous Glucose Monitoring System and Insulin Pump [11]

- **Supervisory Control and Data Acquisition (SCADA)Systems:**TheSupervisory Control and Data Acquisition (SCADA) systems that are used to manage industrial control equipment and critical infrastructure are part of the IoTdevices that are vulnerable as many SCADA systems are now network-enabled but lack efficient security controls by using hard-coded passwords and poor patching processes. Also, Industrial controllers (SCADA) systems that have been in place and are difficult to update are specifically vulnerable for attacks. Attackers could use compromised SCADA systems in DDoS attacks or in ransomware attacks.

- **Baby Monitors:**Consumer products that are used to monitor babies are another category of IoT devices that are vulnerable to attacks and compromise. Some vulnerabilities associated with baby monitors includes: hard-coded passwords, unencrypted communications, privilege escalation, easily guessable passwords, backdoor accounts, and flaws that would have let an attacker alter device functions[12].These vulnerabilities let attackers hijack video sessions, or view video stored in the cloud, or gain complete administrative control of the baby monitor. All of the flaws were easy to exploit and would have given attackers varying degrees of remote control over compromised devices. This vulnerable device could pose a threat to any computer connected to the home network, including those used by remote workers. An infected IoT device could be used to pivot to other devices and traditional computers by taking advantage of the unsegmented, fully trusted nature of a typical home network.

Baby monitor [13]

- **Connected Cars:**MostModern cars are part oftheIoT devices as theirnumerous components are network-accessible and exposed to network-borne threats.The weaknesses in the controller area network of a Jeep Cherokee could be exploited to gain remote control of the vehicle's accelerator, breaking, and steering systems. Other threat in connected cars includes proof-of-concept attacks on Toyota and Ford models.

Connected cars in the Internet of Things Network [14]

1. Vulnerabilities in Internet of Things Network

Vulnerabilities in Internet of Things Network are the security flaws in internet of things that allows an attack to be successful. Some common internet of things vulnerabilities includes:

- **Insecure Internet of Things Network Interface:** Most Internet of Things (IoT) network user over-relies on default password, weak password or using lax password recovery functionality. Other features leading to insecure web interface includes cross-site scripting, cross-site request forgery as well as SQL injection.
- **Insufficient Authentication/Authorization:** Any person or bot accessing the web interface poses some risk. One of the most recognizedthreatsisthat of unauthorized usersaccessingthenetwork interface. To adequately protect information on the internet of things network, authentication and authorizationmust be sufficiently improved.Such authentication and authorization should equally be revokedwhen necessary. It is important toensure that application, device, and server authentication are required using a unique authentication tokens or session keys.

- **Insecure Internet of Things Network Services:** In order to secure the internet of things network services, all the network device's open ports must be analyzed andconfirmedthat they are not vulnerable to cyber-attacks.

- **Lack of Transport Encryption/Integrity Verification:** To reduce this vulnerability, the network traffic, mobile applications as well as other connections should not pass any clear text along the transport layer.To achieve this, the encryption protocols should be ensured, secure sockets layer (SSL) should be used and transport layer security (TLS)must be updated.

- **Insecure Cloud Interface:** in order to securethe cloud interface, network users must avoid usingdefaultusername and passwords, block user accounts that could not login after a predefined number of attempts and also check all the cloud interfaces for any other form of vulnerabilities.

- **Insecure Mobile Interface:** To ensure better security for mobile interface,two-factor authentication security principle should be employed in order to check exposure of data when connected to wireless networks.

- **Lack of proper Security Configuration:** Security configuration should be strengthened through diverse method such asgranting different level of access privileges to different users, encryption, use of very strong password, and recording of different security events for easy intrusion detection.

- **Insecure Software/Firmware:** One of the first priorities here is to ensure that the IoT device can be updated and the update files should be encrypted and transmitted using an encrypted connection. This update should be signed and verified and the update server be secured.

- **Poor Physical Security:** Physical security can equally enhance vulnerability in the IoT network. Storage medium should be secure from easy removal, stored data be encrypted, prevent bad actors from gaining access to the ports as well as ensuring that the device cannot be easily disassembled

2. Attacks Associated to Internet of Things (IoT)

Many types of attacks have been around for a very long time. However, the scale and relative simplicity of such attacks in the Internet of Things (IoT) are now alarming.The numerous devices connected over the internet of things network are prospective targets to common types of cyber-attacks. It fundamentally aims at persistent connection and networking of devices that has not certainly been connected over network. This large number of devices that consistently been connected over this network creates a new entry point to the network and further increases the security and privacy risk of the entire network.The various network attacks and how they affect the internet increases to an extraordinary level with the introduction ofIoT as discussed below.

- **Botnets:**These are network of systems joined together in order to remotely control and distribute malware. It can equally be seen as a collection of internet-connected devices, which may include PCs, servers, mobile devices and internet of things devices that are infected and controlled by a common type of malware [15].It is controlled by botnet operators via Command-and-Control-Servers (C&C Server), they are used by criminals on a grand scale for many things: stealing private information, exploiting online-banking data, DDos-attacks or for spam and phishing emails.Withincreasein internet of things network (IoT), a lot of objects and devices are liable to, or already part of thingbots. A thingbotis a botnet that incorporates separately connected objects. Both botnets andthingbotscontain several different devices connected to oneanotherlikecomputers, smartphones tablets among others.

- **Man-In-The-Middle Internet of Things Network Attack:**This is a type of network attack where the attacker or intruder is concerned with interrupting and breaching an interaction between two separate network devices. It is a very hazardous attack as the attacker secretly interrupts and communicates messages between two parties while both parties felt that their communication is still directly to one another. The intruder directly grasp the original message and send his own fake message to the recipient and makes the recipient to think that he is still getting a legitimate message from the original source. Many cases have already been reported for IoT within this threat area, cases of hacked vehicles and hacked smart refrigerators [16].These attacks can be extremely dangerous in the IoT, because of the nature of the "things" being hacked. Some of the extremely dangerous internet of things devices that can be hacked includesrefrigeratorsindustrial tools, smart TVs, machinery, vehicles and other harmless connected "things" like garage door openers.

- **Data and Identity Theft internet of things network attack:**Mostoften, the internet users constituted thegreatest security enemy to themselves as they insensitively safe keep theirinternet connected devices such as computer, mobile phone, smart watch among others. Hackers can easily take advantage of these devices to launch an identity theft. Themethod used in identity theft is simply to collect data from unauthorized source. The large amount of data on the internet and other daily devices we us can greatly expose our personal identity to hacker. The greater thedetail that hackers obtained about an internet user, the simpler it is to launch a successful identity theft on him.

- **Social Engineering:**Social engineering is the act of manipulating people in order to obtain they confidential information such as passwords, bankinformation or by accessing a computer in order to secretly install malicious software that grants access to personal information and overall control over the computer. Normally, social engineering attacks are carried out using phishing emails, to discloserelevantinformation or redirects users to some important sites such as financial institution or e-commerce websites that look genuine in order to tantalize them supply theirimportant personal details.

- **Denial of Service (DoS) attack**: This is a type of internet of things network attack that truncates a service that is usually available from its target. It is regarded as a Distributed Denial of Service (DDoS) attack, when numerous systems maliciously attack one target system to prevent it from rendering its usual service to the users. The distributed denial of service attack is normally achieved using botnet, where a lot of network devices are programmed to simultaneously request for a service from the target system.Prominentamong this was the series of Distributed Denial of Service (DDoS) attacks that causes a widespread disruption of legitimate internet activity in the US [17]. Theattacks were successful as a result of numerousunsecured internet-connected digital devices, like refrigerators, homerouters,surveillance cameras among others. The intruders use a large number of this network devices that had already been infected with malicious software to produce the botnet.

Distributed Denial of Service (DDoS) attack in IoT [17]

3. Intrusion Detection in Internet of Things

Intrusion Detection Systems (IDS) are strategies or codes that observe network traffics and other system activities for malicious acts or abusesof regulatory policies and send feedback to a management end for possible analysis. It examines all traffics that are either coming in or leaving the network and findsdistrustfulconfigurations that indicatesanintrusion. Some known categories of intrusion detection system include:

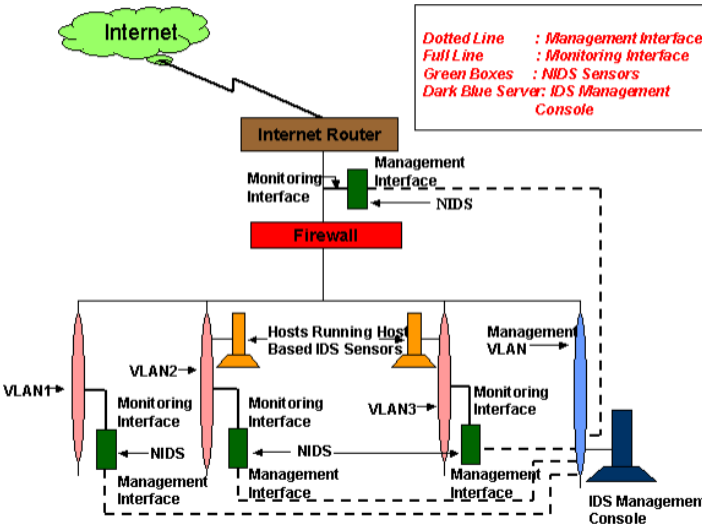
- **Misuse Detection:**Thisis a category of intrusion detection system that evaluates and analysesits generated

information and matches it with the available attack signature's databaseto look for a particular attack that has already been recorded. The efficiency of misuse detection software is determined by the database of attack signatures that it uses.

- **Anomaly Detection:**this is a category of intrusion detection system where the system administrator describes the starting point of network's traffic load, protocolandthetypical packet size. The anomaly detection software checks the network segments andcompares their state to the normal starting point and determine any available irregularities in the network

- **Host-based intrusion detection system:** Inthis category of intrusion detection system, the detection software examines the activities on every host machine such aschecking of the system's configuration files to spot out all inexpedientsettings,checking of the password files to spot outinexpedient passwords as well aschecking of all other system areas to spot outabusedrules.

- **Network-basedIntrusion Detection System (**NIDS**):**This is a category of intrusion detection system where every transmitted packet through the network isproperly analysed. The NIDS can detect harmful packets that are calculated to be ignoredby a firewall's filtering guidelines.A network based IDS sensor has two interfaces [18] and one of them is manageable. The IDS management console communicates with the sensor through the management interface. The other interface of the IDS is in promiscuous (listening) mode and is not accessible over the network hence not manageable. The observing interface is linked to the network section that is being observed. The sensor observes each packet that crosses the network section. Network based sensors apply known attack signatures to every frame to detectantagonistic traffic. If it detects a match against any signature, it alerts the management console.



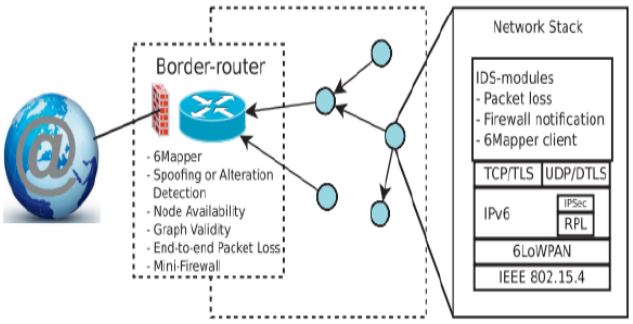
Deployment of IDS Sensors and Management Console in a network [18]

- **Passive intrusion detection system**: In a passive system, the intrusion detection system (IDS) sensor detects a potential security breach, logs the information and signals an alert on the console or owner.

- **Reactive intrusion detection systems**In a reactive system, the IDS responds to the suspicious activity by logging off a user or by reprogramming the firewall to block network traffic from the suspected malicious source.

3. PROPOSED INTRUSION DETECTION METHODS FOR IOT

- **SVELTE intrusion detection system:** This a lightweight and effective IDS First designed specially for IOT [2]. It have an integrated firewall, it consists of6LoWPAN Mapper that Get the information about network and construct it using RPL (IPv6 routing Protocol).Itdetects intrusion by analyzing the mapped data.



SVELTE IDS in IoT [2]

- **An Automata Based Intrusion Detection Method:**This is a uniform intrusion detection method for the vast heterogeneous IoT networks based on an automata model. This method can detect and report the possible IoT attacks with three types: jam-attack, false-attack, and reply-attack automatically [19]

- **Hybrid Intrusion Detection method:**Thismethod of intrusion detection in internet of things was proposed by Sedjelmaci et al In [19] based on the use of Game Theory. This method mixed the usage of signature and anomaly ways for IoT intrusion detection. It achieve this by creating the game model of intruder and normal user.

- **Complex Event-Processing IDS**: which is a Real-time pattern matching system for IoT devices was proposed by J. Chen and C. Chen.Thismethod uses the Complex Event Processing (CEP) that focuses on the use of the features of the events flows to judge the intrusions, which can reduce the false alarm rate comparing with the traditional intrusion detection methods.

- **Artificial Neural Network (ANN) Intrusion Detection System:** Here a multi-level perceptron, a type of supervised ANN, is trained using internet packet traces and was assessed on its ability to thwart Distributed Denial of Service (DDoS/DoS) attacks on IoT devices [20].The detection was based on classifying normal and threat patterns. It was able to identify successfully different types of attacks and showed good performances in terms of true and false positive rates.

4. CONCLUSION

Intrusion detection in internet of things network is established in response to the growing number of intrusions on major websites and networks. To ensure network security in internet of things has become very difficult over the years as a result of larger number of things been connectedandthe high sophisticated nature of attacktechnologies in use. This research presents an overview of intrusion detection in internet of things as well as detail knowledge of various threats, vulnerabilities, attacks and available methods of detecting an intruder in our internet of things network.

REFERENCE

[1] Mohamed Abomhara&Geir M. Køien, 2015, "Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks" Department of Information and Communication Technology,University of Agder, Norway

[2] ShahidRazaa,_, Linus Wallgrena, ThiemoVoigta,baSwedish, "SVELTE: Real-time Intrusion Detection in the Internet of Things"available at http://www.cs.umanitoba.ca/~comp7570/assets/media/0404Singh_M.pdf accessed on 15th/05/2017

[3] Adam Kliarsky, (2017), "Detecting Attacks Against The 'Internet of Things"

[4] PavanPongle, GurunathChavan , (2015), "Real Time Intrusion and Wormhole Attack Detection in Internet of Things" International Journal of Computer Applications, Volume 12.

[5] Tariqahmad Sherasiya1, Hardik Upadhyay2 &Hiren B Patel3, (2016), "A Survey: Intrusion Detection System For Internet Of Things", International Journal of Computer Science and Engineering (IJCSE), Vol. 5, Issue 2, page: 91-98

[6] Nicholas J. Puketza, Kui Zhang, Mandy Chung, Biswanath Mukherjee and Ronald A. Olsson, (1996), "A Methodology for Testing Intrusion Detection Systems" Department of Computer Science University of California, Davis Davis, CA 95616 Second revision.

[7] SMART GRID SOLUTION available at https://www.business.att.com/enterprise/Service/internet-of-things/smart-cities/iot-smart-grid/ accessed on 14th /05/2017

[8] Http://www.darkreading.com/endpoint/7-imminent-iot-threats/d/d-id/1327233?image_number=2Accessed on 15th /05/2017

[9] http://www.darkreading.com/endpoint/7-imminent-iot-threats/d/d- id/1327233?image_number=3Accessed on 13th/05/2017

[10] Rishabh S. Khosla, Pranul S. Chheda, Smith R. Dedhia, Dr.BhaveshPatel , (2016), International Journal on Recent and Innovation Trends in Computing and Communication, Volume: 4 Issue: 1, Shah & Anchor Kutchhi Polytechnic, Mumbai, India

[11] Hacking Implantable Medical Devices, (2014), available at http://resources.infosecinstitute.com/hcking-implantable-medical-devices/ Accessed on 15th/05/2017

[12] http://www.darkreading.com/endpoint/7-imminent-iot-threats/d/d-id/1327233?image_number=7Accessed on 13th/05/2017

[13] AAMIR LAKHANI , HACKING, (2016), "WHEN BABY MONITORS ARE A MODEL FOR IOT SECURITY", available at http://www.drchaos.com/when-baby-monitors-are-a-model-for-iot-security/Accessed on 15th/05/2017

[14] MR. SHASHANK DHANESHWAR, (2015), "INTERNET OF THINGS APPLICATION FOR CONNECTED VEHICLES AND INTELLIGENT TRANSPORT SYSTEMS", Available at https://www.slideshare.net/shashankdhaneshwar/iot-applications-for-connected-vehicle-and-its accessed on 13th/05/2015

[15] http://searchsecurity.techtarget.com/definition/botnet

[16] "5 Common Cyber Attacks in the IoT - Threat Alert on a Grand Scale" (2016),

[17] STEPHEN COBB, (2016), "10 things to know about the October 21 IoTDDoS attacks" Available at https://www.welivesecurity.com/2016/10/24/10-things-know-october-21-iot-ddos-attacks/ accessed on 15th/05/2017

[18] SANS Institute 2001, Intrusion Detection Systems: Definition, Need and Challenges, available on https://www.sans.org/reading-room/whitepapers/detection/intrusion-detection-systems-definition-challenges-343

[19] Yulong Fu, Zheng Yan, Jin Cao, Ousmane Koné and Xuefei, (2017), "An Automata Based Intrusion Detection Method for Internet of Things" available at https://www.hindawi.com/journals/misy/2017/1750637/ accessed on 13th/05/2017

[20] Elike Hodo, Xavier Bellekens, Andrew Hamilton, Pierre-Louis Dubouilh, Ephraim Iorkyase, Christos Tachtatzis and Robert Atkinson, "Threat analysis of IoT networks Using Artificial Neural Network Intrusion Detection System", available at https://arxiv.org/ftp/arxiv/papers/1704/1704.02286.pdf accessed on 15th/05/2017

[21] Gemalto solutions, (2017), "Securing the Internet of Things (IoT)", available at https://safenet.gemalto.com/data-protection/securing-internet-of-things-iot/ accessed on 2nd/05/2017

[22] "The 10 Biggest IoT Security Vulnerabilities Brian Buntz", (2017), available at http://www.ioti.com/security/10-biggest-iot-security-vulnerabilities accessed on 5th/05/2017

[23] "Design of Complex Event-Processing IDS in Internet of Things" available at http://ieeexplore.ieee.org/document/6802673/ accessed on 10th/05/2017

[24] JAI Vijayan, (2016), "7 Imminent IoT Threats" available at http://www.darkreading.com/endpoint/7-imminent-iot-threats/d/d-id/1327233accessed on 12th/05/2017

[25] http://www.darkreading.com/endpoint/7-imminent-iot-threats/d/d-id/1327233?image_number=4 ACCESSED ON 14TH/05/2017

[26] http://www.ioti.com/security/10-biggest-iot-security-vulnerabilities/gallery?slide=1 ACCESSED ON 15TH/05/2017

[27] http://www.ioti.com/security/10-biggest-iot-security vulnerabilities /gallery?slide=2 ACCESSED ON 13TH/05/2017