ISSN: 0974-5823 Vol. 7 No. 4 April, 2022

International Journal of Mechanical Engineering

Internet of Things Security: Challenges and Solution

Vibha Mani,VM,Mani

Computer Science Dept.

Jaypee Institute of Technology,Sec-128 NOIDA

Dr. Charu, DC

Computer Science Dept.

Jaypee Institute of Technology,Sec-128 NOIDA

Dr. Shruti Jaiswal, SJ, Jaiswal

Computer Science Dept.

Jaypee Institute of Technology,Sec-128 NOIDA

Abstract: From the last one to two-decade information technology is growing like a global giant. A rapid growth is seen in IoT platforms in the last one decade. Internets of Things (IoT) devices are easy to handle and are easily accessible which make them available to everyone at any location. Because of fast growing demand for smart devices and their easy availability IoT system, leads IoT to face more security challenges than ever before. In this paper our primary focus is to define security attacks that are occurring in devices and their networks which are related to IoT. The paper discusses various IoT attacks happening around, classifying them according to IoT layers. Thereafter, various counter measures available to implement the identified attacks are presented.

Keywords: Internet of Things Layered Architecture, Security Attacks, Solution of security attack, Machine learning.

1. INTRODUCTION

Word “internet of things” was first raised by Kevin Ashton in 1999; he was giving a presentation for P & G supply chain in link with RFID where he introduced “Internet of Things“first time [1]. IoT is a concept by which machines can interact with each other without the intervention of human beings [2]. In IoT device to device communication occurs and these devices work in coordination with each other to perform particular tasks. Nowadays IoT is everywhere such as in healthcare, transportation, automobile industries, smart homes [3]. Definition of the IoT given by International Telecommunication Union(ITU) as “ a global infrastructure for the information society , enabling advanced service by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies” [4]. As the IoT system is evaluated it starts facing many kinds of issues such as standardization of architecture, communication protocol and security [2].figure 1 show how the world around us changes from human to human interaction to machine to machine interaction over a period of time [5].

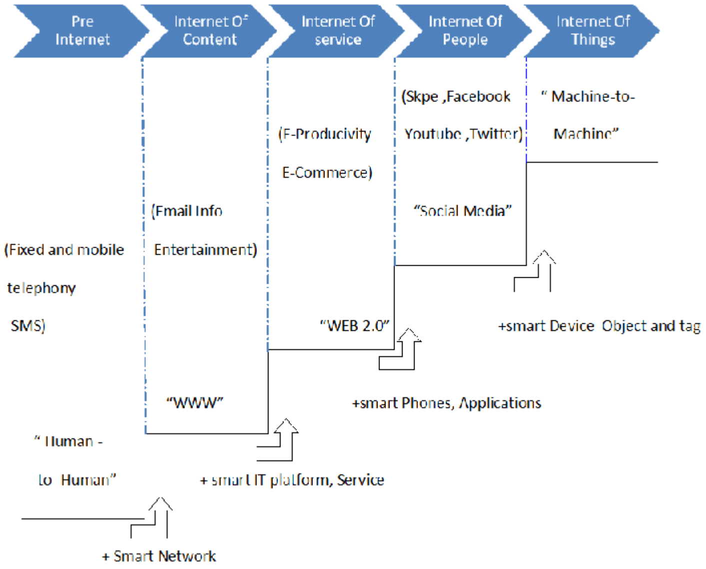
Pre Internet
Internet Of Content
Internet Of service
Internet Of People
Internet Of Things
(Skpe ,Facebook Youtube ,Twitter)
“ Machine-to-Machine”
(E-Producivity E-Commerce)
“Social Media”
(Email Info Entertainment)
(Fixed and mobile telephony SMS)
“WEB 2.0”
+smart Device Object and tag
“WWW”
+smart Phones, Applications
“ Human - to Human”
+ smart IT platform, Service
+ Smart Network

Figure 1: Evolution of IoT

In today's world the internet of things becomes a respiration process, it is everywhere such as smart phone, smart watch, smart lights, fridge, microwave, computers, cars etc. It integrates various devices to network and provide services to the user which make their life much easier. But! At what cost? Yes! The question is: How IoT protects user privacy and address from attacks. In this paper we are trying to classify attacks according to IoT system architecture and services and then we focus on existing solutions present to counter these attacks. [6-8].

The paper is prepared as follows. Section II is the overview of layered architecture of the IoT system. In section III we discuss each layer of IoT and attacks on corresponding layers. Section IV examines existing solutions for those attacks. Section V concludes the paper.

2 LAYERED ARCHITECTURE OF IoT

IoT architecture is defined in different layers; each layer is defined by its function and devices that are used in each layer. There are different views of researchers about the number of layers in IoT. However, according to most of the researchers IoT essentially works on three layers [9-11].It was presented at an early stage of research in IoT and still most valid architecture [12]. For the research proposed scientists claim that three layered architecture is not sufficient for finer aspects of IoT [12, 13]. That's why there are many other architectures proposed by researchers. In this paper our center of attention is on three layered architecture of IoT, which has perception, network and application layer as shown in fig 2.

Perception Layer: It shows how data sent over network by the use of physical medium such as cables, wires. In this layer we use sensor and actuators for sensing and gathering information. This layer is also recognized as the physical layer of IoT.

Network Layer: This layer is accountable for sending IP datagram from source network to target network. In other words this layer is responsible for connection of network devices and server.

Application Layer: Application layer provide a medium of interaction between various applications and lower layer of the architecture. It provides application specific services and sends data over the network.

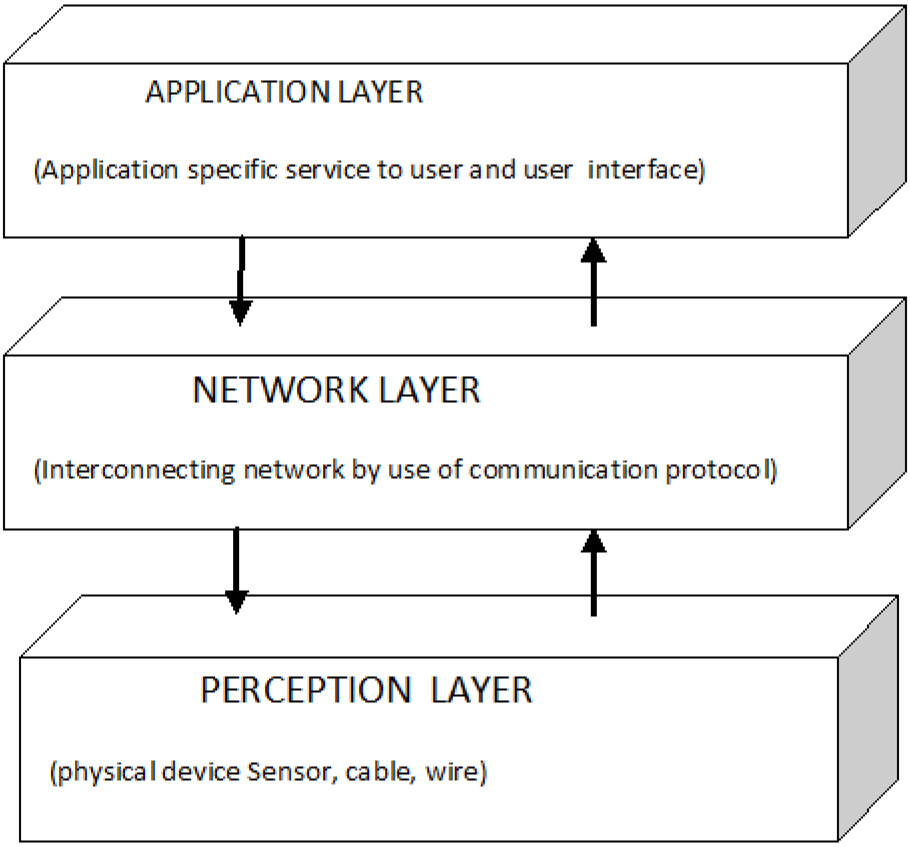
APPLICATION LAYER
(Application specific service to user and user interface)
NETWORK LAYER
(Interconnecting network by use of communication protocol)
PERCEPTION LAYER
(physical device Sensor, cable, wire)

Figure 2: Three Layered architecture of IoT

3 SECURITY ATTACK ON DIFFERENT LAYER OF IoT

Now a days we can see more and more device are connected to the internet because of high adoption rate of IoT. As adoption is high the smart devices are becoming target for information risk. It is worth notice and examines security attack according to IoT layer and protocol used in each layer. As Gartner said in his insides paper “By 2020 more than 25%of identified attacks in enterprise will involve the IoT, although the IoT will account for less than 10% of IT security budgets” [14].

3.1 Security attack on application layer

At application layer service, data and application are works in huge and composite cluster and in the cloud computing environment , because of this it can be affected by many attacks and vulnerabilities(SQL injection, permission access, buffer overflow, cross site scripting, simple password) such as data tempering , authentication to server, authorization of data provisioning etc.[15]

Denial of service attack nodes can easily trap and attackers can demolish the accessibility of the application or service or data. In privacy leaks users can easily steal user data. The attacker can also examine incurable location and individuality isolation by the query result. Attackers can upload malicious code leading to software infection. If there is a relationship between users of IoT then the attacker can simply examine or gain extra information which in future can be used for social engineering attack [16].

3.2 Security attack on Network layer

Network is a place which is always busy with a large amount of data travelling through a network layer. Because of this network layer has high security thread possibility and it leads to network overcrowding [17]. Integrity and authentication of data which is transported in the network are hampered by attackers in this layer. Some common intimidation in network layer are DoS, DDoS, Malicious code injection ,MIMT and Replay attack [18].

In DoS bombardment of data request is done by the attackers so that the system , server or network exhaust their resources and bandwidth to fulfill the request and do not do the main work. Sometimes the whole system crashes due to DoS attacks. If there are more than one system involved in an attack then it is known as DDos(Distributed Denial of Services). In Reply attack, the attacker intercepts and saves old messages and then tries to send them later, impersonating one of the participants. Men in the middle attacks are the most common type of security attack in which the attacker listens to communication between the two communicating hosts. The attacker inserts themselves into two party transactions and then they can easily interrupt the traffic, strain and whip data. Most of the time MIMT attacks used unsecure wi-fi and malware software as their entry point. In malicious code injection attacker inject malicious code in the working code to authorize access control on the network [12].

3.3 Security attack on perception layer

This layer is used for collecting information from sensor devices and controlling the system's physical component. At perception layer smart devices enabled with microcontroller fit for IoT application and have interface with actuators and sensor. There are many types of security thread at this layer which are serious concern [19].

In a node capture attack, a hacker captures a node or replaces it with a new/fake node. By analyzing the node, hackers can get confidential information like security key, access authorization etc. fake nodes can work as malicious nodes according to the direction of the attacker.

Malicious code injection is another type of attack on the perception layer in which malicious code is transferred to the node memory by using restores modules. By use of malicious code, hackers can tamper or slow down the overall network. False data injection attack is also like a malicious code injection attack. In this erroneous data injected through tempered nodes that leads to malicious activity in delivery of service to the consumer. In eavesdropping, the attacker secretly or stealthily performs leakage in the communication channel either by wire line or wireless. It can lead to DoS attacks. Sleep deprivation attack is like DoS attack. It drains out or exhausts the battery content of the edge device either by harming hardware or by malicious code injection into node memory. In booting vulnerabilities, attackers attack on the device in the booting phase, when most of the security mechanisms are not enabled. Attackers try to get sensitive data or inject some malicious code in the system [20].

Hardware exploitation is tempering debug ports, on-chip instruments, JTAG used for debugging and obtaining a right of entry to private assets of the edging device. Similarly software exploitation is tempering embedded software to access confidential data.

Following table summarized the above discussion. In this table the first column used to take different layers of IoT. Protocols used in different layers come in the protocol column. The next column used to table security attacks according to each layer. And in the last column security parameters which are affected by the security attack are considered.

Table 1: IoT Layers with related Protocol, Security Attack and Security Parameter

IoT Layer	Protocol	Security Attack	Security Parameter
Application Layer	MQTT, REST, CoAP, AMQP, HTTP, WebSocket ,DSS	DoS, Malcious Code, Privacy leak, Social Engineering [15]	Data Privacy, Access Control, Confidentiality, Integrity
Network Layer	IPv4,IPv6,6LoWPAN	DoS, DDoS ,Reply Attack, MITM attack, Malicious code injection[18]	Authentication, Integrity
Perception Layer	Ethernet, WiFi,LR-WPAN, 2G/3G/4G Mobile communication	DoS, Malicious code injection, False data Injection attack, Side Channel attack, Node Capture attack, Eavesdropping and interference, Sleep Deprivation attack, Booting Vulnerabilities, Hardware Exploitation, Software exploitation [20]	Integrity, Authentication, Confidentiality[18]

Many different scientists have different opinions on security attacks which make the list endless. In this paper we consider only layered architecture and attack on the layers. In the next part of the paper we try to elaborate the existing solution on this type of attack.

4 EXISTING SOLUTION

As IoT devices used to correspond with each other without or minimum human communication, the security parameters like authentication and access control become a significant part of the standard. Most of the IoT devices gather our personal data because of that, devices should be able to control remotely and must be lashed with high security and protection [18]. In this section we are going to compare existing security solutions proposed by different literatures which are discussed in Table.

4.1 Existing solution for Application Layer

Most frequent hit in IoT platforms is done by Denial of Service attack. In DoS attacks a huge amount of data request is sent on the application layer so that the system will be busy in fulfilling the request and avoid other important work which creates passage for the hackers. In this paper DoS attack detection structure for MQTT attack detection in IoT is projected and estimated [21]. For the effectiveness test of the proposed feature author used three machine learning algorithms which are AODE based on Naïve Bayes, C4.5 based on detection tree and MLP based on an ANN. The proposed MQTT feature has high detection capacity, high memory utilization and is also used for detecting Dos attacks in IoT networks. Privacy leak is a type in which user personal data or confidential data is leaked in the application layer by query or massage. Monique Bezuidenhout et al proposed a model named SEADM (Social Engineering Attack Detection Model) by using decision tree [22]. To present the model and for analysis of the potential threat authors took different kinds of scenarios. As the result shown, we can say that SEADM is a user friendly and practically applied help or assistantship for daily awareness of threats which are actually protecting us from social engineering attacks.

Authors gives a data leak detection model with its insights [23].They implemented a fuzzy fingerprint framework in Python. The framework includes packet collection, shingling, Robin fingerprinting, partial disclosure and fingerprint filter extension. They used the organizer (i.e. data owner) and Data Leak Detection (DLD) provider as a key player in the fuzzy fingerprint model. They have done experiments to authenticate the efficiency, accuracy and privacy of their solution. Yuancheng Li et al propose a malicious code detection scheme based on Auto Encoder and DBN (Deep Belief Network) [24]. They used a dataset of KDDCUP'99 for the authenticity of the model. The model mechanism is in two steps; in first step it uses Auto Encoder to extract main features of data then in second step use DBN to detect malicious code. The result shows improved detection accuracy, while reducing the time complexity of the model as compared to single DBN.Authors gives a data leak detection model with its insights [23].They implemented a fuzzy fingerprint framework in Python. The framework includes packet collection, shingling, Robin fingerprinting, partial disclosure and fingerprint filter extension. They used the organizer (i.e. data owner) and Data Leak Detection (DLD) provider as a key player in the fuzzy fingerprint model. They have done experiments to authenticate the efficiency, accuracy and privacy of their solution. Yuancheng Li et al propose a malicious code detection scheme based on Auto Encoder and DBN (Deep Belief Network) [24]. They used a dataset of KDDCUP'99 for the authenticity of the model. The model mechanism is in two steps; in first step it uses Auto Encoder to extract main features of data then in second step use DBN to detect

malicious code. The result shows improved detection accuracy, while reducing the time complexity of the model as compared to single DBN.

4.2 Existing Solution for Network Layer

Detection of Light weight replay attack for battery dependent IoT device [25] was proposed by Paveen et al. Replay attack recognition was done on Android platform and within 20 seconds the solution shows the unusual activity if any. The system also sends an alert message warning about the attack. The overall solution proposed by authors found consistent and precise as it shows detection of replay attack in 20 sec and after that work normally. Hitesh Mohapatra et al proposed MITM-IDS [26] for recognition of attack, then isolation of the node and reconfiguration for attacked nodes. The proposed model output is validated by considering two factors first is packet loss and second is throughput. As the result shows the system successfully detects attacks and fraudulent activity which enhance the overall performance of the network with high throughput and low packet loss.

Intrusion checkers is work proposed by Devu Manikantan Shila et al [27]. In this approach intrusion checker first learns the behavior of each procedure call which is in the training stage (offline phase) of firmware and secondly it uses the learned skill to detect any malicious deviation of the procedure behavior. The result of intrusion checkers shows detection of attack with 100% accuracy. Authors [28] proposed an ADE (Average Dependence Estimators) based Dos attack detection scheme for IoT sensors.A1DE are probabilistic data classification techniques based on the Naïve Bayes Classifier. A2DE classifier allows the establishment of a dependency between the class attribute and two other features. They used integration of A1DE and A2DE through the introduction of Multi Scheme and Voting Scheme for detection of DoS attack in IoT network. Performance of A2DE was best as compared to other classifiers or the IoT database that was tested. An IoT DDoS defense algorithm for an IoT network is proposed for prevention and avoidance from DDoS attack by Zhang et al [29]. They used a working node as a device which collects information and executes simple tests in an IoT network. To defend itself from DoS attacks a working node will be able to distinguish malicious requests from legitimate one. The sender flagged as an attacker if he sent requests with the same content repetitively. COOJA network simulator is used for this purpose and results show that the algorithm successfully works on the working node of a network to differentiate malicious requests from genuine one.

4.3 Existing Solution for Perception Layer

Fan Ye et al developed a model named SEF (Statistical En-Route Filtering) for false report detection [30]. There are two main goals of SEF, firstly early detection of false data information and secondly low computation and communication overhead. Analysis and simulation show that SEF decreases 70% false report injection by compromised nodes within five hopes and for ten hopes 90% along the forwarding path. Yair Meidan et al proposed a model for detecting IoT attack works on deep autoencoders for every device, which is skilled on statistical features obtained from benign traffic data [31]. The method consists of four main stages: data collection, feature extraction, training and anomaly detection and continuous monitoring for anomaly detection. The experiment result for most IoT devices obtained FPR (false positive rate) as zero in the test set.

Rafique et al proposed a solution for plausible risk of (CFA) crossfire attack on SDN (Software Defined Network) for IoT edge model [32]. CFA is a type of DDoS attack which employs a roundabout strategy to attack an object server. The work is divided into different modules: Link selection module, Attack detection module, malicious flow interception module. The experiment results show a defense solution against CFA. The results demonstrate that CFA Defense precisely detects and defines CFA with minimum performance overhead on the network. Farah kandan et al proposed a solution for MANET by injecting malicious nodes into a network as a defense of colluding injected attacks (CIA) [33]. The purpose of this malicious node is to hide its identity from legitimate nodes and effort together to produce rigorous network attacks, which try to make an impact at a random node, by which attacked node will be unable accept or transmit any packet when it is identified as malicious. The main purpose of this model is, for the whole network it can detect exact malicious nodes which were not possible in the previous model. As a result shown in the true detection ratio CIA, MOVE schemes are much better than BLM (Basic Local Monitoring) and MCC (Mitigating Colluding Collision) attacks.

When a malicious node pushes legitimate nodes, forcefully throws away their force or power by resisting the sensor node to go to low power sleep mode and then this scenario is known as sleep deprivation attack. Tapolina Bhattasali and Rituparna Chaki proposed a light weight model INSOMNIA MITIGATING INTRUSION DETECTION SYSTEM (IMIDS) to detect insomnia os stationary sensor node for heterogeneous wireless sensor network (HWSNET)[34]. Performance analysis is done by using simulation in MATLAB. The result of simulation shows energy consumption is compared with respect to the density of sensor nodes with clusterization and sectorization and without clusterization or sectorization comparison is done in the existing Isolation Table Intrusion Detection System (ITIDS) and proposed IMIDS. Authors [35] proposed a representation to formalize location privacy issues under a global eavesdropper and anticipated the minimum average communication overhead needed to achieve a particular level of privacy. To protect global eavesdropping they present a technique which provides location privacy to objects. For protecting location information of objects and also to protect data sink, authors provided a homogeneous sensor network model and proposed privacy preserving technique. To estimate energy spending and latency they used simulation.As the result shows that highest location privacy can be achieved by periodic collection method and they are useful when we are monitoring highly valuable objects.

Consumer electronic devices were digitized and they also inherit the digital world security vulnerabilities, side channel attack is one of those vulnerabilities in which covert data outflow with compromised private key implanted within the device.

Jungmir Park and Akhilesh Tyagi address side channel attack and proposed power side channel as a solution [36]. Machine learning classifier is used to address different types of side channel attack and AVR microcontroller which are based on side channel disassemble are used to extort assembly level code by the side of the control flow graph from side channel leakage. As result shown, with more than 80% accuracy instruction level disassembly of an AVR microcontroller are capable of spotting an intrusion in the power side channel. Mouro Conti et al proposed a distributed solution to node capture detection for wireless sensor network [37]. They used mobility based node capture detection in which they use two protocols SDD (Simple Distributed Detection) and CDD (Cooperative Distributed Detection) to prevent network from node capture attack by detecting attack as soon as possible. The simulation results show the protocol works perfectly in certain conditions.

Congmiao Li et al proposed hardware exploitation attack detection by monitoring micro architectural feature deviation [38]. They used this feature to detect Spectre (exploits speculative execution and side channel vulnerability) and Rowhammer(exploits DRAM disturbance error vulnerability) attack. Hardware performance counters are used to collect the features of micro architecture. To detect malicious behavior at an early stage of attack they used an online detection method. Results show accuracy rate for Rowhammer attack 0.77% false positive and for Spectre attack 0% false negative. S. Velliangiri et al proposed detection scheme for DDoS attack to detect intruder nodes in the cloud surroundings [39]. They used a deep learning strategy for important information enclosed in the cloud platform. The simulation was done on TEHO-DBN (Taylor-Elephant Herd Optimization Based Deep Belief Neural Network) classifier for finding attack and their results are observed for 3 different databases. The results show accuracy of detection 83, rate of detection 89% precision in detection 89% and 89% recall.

Table 2: Existing solutions for different attacks at IoT layers

Layer	Attack	Proposed Solution
Application Layer	DoS,	Proposed a framework for detection of MQTT attack in Dos attack[21]
	Malcious Code	Malicious code detection scheme based on Auto Encoder and DBN(Deep Belief Network) [24]
	Privacy leak	Data leak detection model by using Fuzzy fingerprint [23]
	Social Engineering	A model named SEADM by using decision tree [22]
Network Layer	Replay Attack	Provided solution for battery depended IoT devices to detect lightweight reply attack. [25]
	MIMT attack	Paper provide a solution for detecting MIMT-IDS attacks[26]
	Malicious code injection	Paper proposed intrusion checkers to protect against malicious firmware attacks [27]
	DoS attack	ADE(Average dependence estimators) based Dos attack detection scheme for IoT sensors[28]
	Distributed Denial of Service(DDoS)	An IoT DDoS protection algorithm to an IoT network is proposed for prevention and avoidance from DDoS attack [29]
Perception Layer	Malicilous code injection	The paper proposed a model for protection from CIA in MANET [33]
	DoS attack	A solution for plausible risk of CFA on software defined network IoT edge model [32]
	Node capture attack	Proposed a distributed solution detect node capture [30]
	Eavesdropping Attack	Paper provided a model to formalize location privacy issue which comes under a global eavesdropper [35]
	False data Injection attack	Developed SEF for false report detection [30]
	Side Channel attack	Provided solution as Power side channel [36]
	Sleep Deprivation attack	A light weight model IMIDS presented for HWSNET to find insomnia of stationary sensor node [34]
	Booting Vulnerabilities	The paper present a detection method for IoT attack on deep autoencoders for each device [31]
	Hardware Exploitation	A hardware exploitation attack detection by monitoring micro architectural feature deviation [38]
	Software exploitation	CFADefense is a software exploitation solution [32]

5 CONCLUSION

In the past few years, IoT has been developed rapidly and large numbers of enabling technology have been proposed. The obstacles in expansion of IoT are known as the security and privacy problem. It is necessary to have security at every layer of IoT for smooth functioning of IoT. There are many studies in IT security and most of them are effectively implemented in security infrastructure of IoT. Machine and deep learning are new and adaptive technology and there is lots of scope of improvement in security of IoT, if they pass their journey hand in hand with each other.

REFERENCES

1. Ashton, K. (2009). That ‘internet of things’ thing. *RFID journal*, *22*(7), 97-114.
2. Li, S., Da Xu, L., & Zhao, S. (2015). The internet of things: a survey. *Information Systems Frontiers*, *17*(2), 243-259.
3. Asghari, P., Rahmani, A. M., & Javadi, H. H. S. (2019). Internet of Things applications: A systematic review. *Computer Networks*, *148*, 241-261.
4. ITU (2012) New ITU standards define the internet of things and provide the blueprints for its development. http://www.itu.int/ ITU-T/newslog/New?ITU?Standards?Define?The?Internet?Of?Things?And?Provide?The?Blueprints?For?Its?Develo pment.aspx. Accessed 27 Sep 2014
5. Dash, A., Pal, S., & Hegde, C. (2018). Ransomware auto-detection in IoT devices using machine learning. *Int. J. Eng. Sci*, *8*, 19538-19546.
6. Rizvi, S., Orr, R. J., Cox, A., Ashokkumar, P., & Rizvi, M. R. (2020). Identifying the attack surface for IoT network. *Internet of Things*, *9*, 100162.
7. El Mouaatamid, O., Lahmer, M., & Belkasmi, M. (2016). Internet of Things Security: Layered classification of attacks and possible Countermeasures. *electronic journal of information technology*, (9).
8. Tawalbeh, L. A., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT Privacy and security: Challenges and solutions. *Applied Sciences*, *10*(12), 4102.
9. 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.
10. 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.
11. Wu, M., Lu, T. J., Ling, F. Y., Sun, J., & Du, H. Y. (2010, August). Research on the architecture of Internet of Things. In *2010 3rd international conference on advanced computer theory and engineering (ICACTE)* (Vol. 5, pp. V5-484). IEEE.
12. Wu, M., Lu, T. J., Ling, F. Y., Sun, J., & Du, H. Y. (2010, August). Research on the architecture of Internet of Things. In *2010 3rd international conference on advanced computer theory and engineering (ICACTE)* (Vol. 5, pp. V5-484). IEEE.
13. Darwish, D. (2015). Improved layered architecture for Internet of Things. *Int. J. Comput. Acad. Res.(IJCAR)*, *4*, 214-223.
14. Hung, M. (2017). Gartner insights on how to lead in a connected world. *Gartner, Inc., Stamford, CT, USA, Tech. Rep*.
15. Nastase, L. (2017, May). Security in the internet of things: A survey on application layer protocols. In *2017 21st international conference on control systems and computer science (CSCS)* (pp. 659-666). IEEE.
16. Zhang, W., & Qu, B. (2013). Security architecture of the Internet of Things oriented to perceptual layer. *International Journal on Computer, Consumer and Control (IJ3C)*, *2*(2), 37-45.
17. Kumar, S. A., Vealey, T., & Srivastava, H. (2016, January). Security in internet of things: Challenges, solutions and future directions. In *2016 49th Hawaii International Conference on*
18. Deep, S., Zheng, X., Jolfaei, A., Yu, D., Ostovari, P., & Kashif Bashir, A. (2020). A survey of security and privacy issues in the Internet of Things from the layered context. *Transactions on Emerging Telecommunications Technologies*, e3935.
19. Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. *IEEE Internet of Things Journal*, *4*(5), 1125-1142.
20. Kumar, S., Sahoo, S., Mahapatra, A., Swain, A. K., & Mahapatra, K. K. (2017, December). Security enhancements to system on chip devices for IoT perception layer. In *2017 IEEE International Symposium on Nanoelectronic and Information Systems (iNIS)* (pp. 151-156). IEEE.
21. Syed, N. F., Baig, Z., Ibrahim, A., & Valli, C. (2020). Denial of service attack detection through machine learning for the IoT. *Journal of Information and Telecommunication*, *4*(4), 482-503.
22. Bezuidenhout, M., Mouton, F., & Venter, H. S. (2010, August). Social engineering attack detection model: Seadm. In 2010 Information Security for South Africa (pp. 1-8). IEEE.
23. Shu, X., Yao, D., & Bertino, E. (2015). Privacy-preserving detection of sensitive data exposure. IEEE transactions on information forensics and security, 10(5), 1092-1103.
24. Li, Y., Ma, R., & Jiao, R. (2015). A hybrid malicious code detection method based on deep learning. International Journal of Security and Its Applications, 9(5), 205-216.
25. Rughoobur, P., & Nagowah, L. (2017, December). A lightweight replay attack detection framework for battery depended IoT devices designed for healthcare. In *2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions)(ICTUS)* (pp. 811-817). IEEE.
26. Mohapatra, H., Rath, S., Panda, S., & Kumar, R. (2020). Handling of man-in-the-middle attack in wsn through intrusion detection system. *International journal*, *8*(5), 1503-1510.

27. Shila, D. M., Geng, P., & Lovett, T. (2016, May). I can detect you: Using intrusion checkers to resist malicious firmware attacks. In *2016 IEEE Symposium on Technologies for Homeland Security (HST)* (pp. 1-6). IEEE.
28. Baig, Z. A., Sanguanpong, S., Firdous, S. N., Nguyen, T. G., & So-In, C. (2020). Averaged dependence estimators for DoS attack detection in IoT networks. *Future Generation Computer Systems*, *102*, 198-209.
29. Zhang, C., & Green, R. (2015, April). Communication security in internet of thing: preventive measure and avoid DDoS attack over IoT network. In *Proceedings of the 18th Symposium on Communications & Networking* (pp. 8-15).
30. Ye, F., Luo, H., Lu, S., & Zhang, L. (2005). Statistical en-route filtering of injected false data in sensor networks. *IEEE Journal on selected areas in communications*, *23*(4), 839-850.
31. Meidan, Y., Bohadana, M., Mathov, Y., Mirsky, Y., Shabtai, A., Breitenbacher, D., & Elovici, Y. (2018). N-baiot—network-based detection of iot botnet attacks using deep autoencoders. *IEEE Pervasive Computing*, *17*(3), 12-22.
32. Rafique, W., He, X., Liu, Z., Sun, Y., & Dou, W. (2019, August). CFADefense: A security solution to detect and mitigate crossfire attacks in software-defined IoT-edge infrastructure. In *2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)* (pp. 500-509). IEEE.
33. Kandah, F., Singh, Y., Zhang, W., & Wang, C. (2013). Mitigating colluding injected attack using monitoring verification in mobile ad-hoc networks. *Security and Communication Networks*, *6*(4), 539-547.
34. Bhattasali, T., & Chaki, R. (2011, July). A survey of recent intrusion detection systems for wireless sensor network. In *International conference on network security and applications* (pp. 268-280). Springer, Berlin, Heidelberg.
35. Mehta, K., Liu, D., & Wright, M. (2011). Protecting location privacy in sensor networks against a global eavesdropper. *IEEE Transactions on Mobile Computing*, *11*(2), 320-336.
36. Park, J., & Tyagi, A. (2017). Using Power Clues to Hack IoT Devices: The power side channel provides for instruction-level disassembly. *IEEE Consumer Electronics Magazine*, *6*(3), 92-102.
37. Conti, M., Di Pietro, R., Mancini, L. V., & Mei, A. (2008, March). Emergent properties: detection of the node-capture attack in mobile wireless sensor networks. In Proceedings of the first ACM conference on Wireless network security (pp. 214-219).
38. Li, C., & Gaudiot, J. L. (2019, July). Detecting malicious attacks exploiting hardware vulnerabilities using performance counters. In 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC) (Vol. 1, pp. 588-597). IEEE.
39. Velliangiri, S., Karthikeyan, P., & Vinoth Kumar, V. (2020). Detection of distributed denial of service attack in cloud computing using the optimization-based deep networks. *Journal of Experimental & Theoretical Artificial Intelligence*, 1-20.