International Journal of Scientific Research & Engineering Trends
Volume 5, Issue 6, Nov-Dec-2019, ISSN (Online): 2395-566X

A Survey of Deep-Learning Model using Intrusion Detection for the Internet of Things

Ms.S.Vinitha Prof. M.Ganesan Ms.S.Arabindhu
Department of Computer Science and Engineering
SMVEC, Pondicherry, India

***Abstract* - Cyber-attacks on the Internet of Things (IoT) are developing at a disturbing rate as gadgets, applications, and correspondence systems are winding up progressively associated and coordinated. At the point when assaults on IoT systems go undetected for longer periods, it influences accessibility of basic frameworks for end clients, expands the quantity of information breaks and wholesale fraud, drives up the expenses and affects the income. It is basic to recognize assaults on IoT frameworks in close ongoing to give powerful security and guard. In this paper, we build up a wise interruption discovery framework custom fitted to the IoT condition. Specifically, we utilize a profound learning calculation to identify pernicious traffic in IoT systems. The location arrangement gives security as an administration and encourages interoperability between different system correspondence conventions utilized in IoT. We assess our proposed recognition system utilizing both genuine system follows for giving a proof of idea, and utilizing recreation for giving proof of its adaptability. Our exploratory outcomes confirm that the proposed interruption recognition framework can recognize true interruptions adequately.**

***Keywords* - Internet of Things (IoT), Intrusion Detection System (IDS), Deep Learning Model.**

I. INTRODUCTION

The Internet of Things (IoT) has developed as the following enormous mechanical transformation in processing as of late with the possibility to change each circle of human life. With an extending system of interconnected Internet-empowered gadgets, IoT gadgets are utilized in a scope of uses from associated vehicles, brilliant homes, human services, keen retail, and store network the board [1][2]. Juniper research predicts that about 38 billion gadgets will be associated with the Internet constantly 2020 [3]. The ascent of this transformative innovation is anyway profoundly soiled with security and protection concerns [4][7].

The huge influx of associated gadgets presents new vulnerabilities and opens new roads for security assaults. To exacerbate the situation, IoT gadgets are regularly made with little respect for security as well as delivered without satisfactory security controls set up. Research demonstrates that a huge level of ebb and flow IoT gadgets available have genuine security flaws and vulnerabilities [8]. Straightforward IoT gadgets can be transformed into assault vectors if not appropriately verified. Ongoing proof of this was seen in October 2016 where hacked IoT gadgets (cameras and DVRs) directed Dyne, the biggest DNS supplier, bringing about enormous Internet blackout, upsetting the accessibility of prominent sites, for example, Twitter, Amazon, and Netflix [9]. All the more as of late, scientists have had the option to cause an auto accident in the autopilot mode [10], showing the vulnerabilities of associated vehicles. New drifts in cyber-attacks (ransom ware, malware) progressively target associated medicinal IoT gadgets bringing about assaults on social insurance organizations, traded off electronic wellbeing record frameworks, or in the direst outcome imaginable, even death toll [11]. Indeed, even with some safety efforts set up, IoT systems are as yet helpless against different assaults because of their huge assault surface. It is consequently fundamental to have the option to structure guard systems fit for distinguishing assaults.

Security barrier estimates, for example, interruption discovery frameworks (IDS) are basic to defenseless IoT situations. Because of inherent asset and computational limitations, customary security techniques can't be legitimately connected to verify IoT frameworks. Existing exploration on interruption location for the IoT is to a great extent concentrated on guideline based recognition methods [12][14]. For efficient discovery of zero-day dangers, oddity based location strategies are fundamental particularly in developing IoT conditions. Additionally, in an IoT biological system, where numerous gadgets are continually producing huge amounts of information, AI calculations can be helpful to perform computerized information investigation and give important elucidations and expectations about the framework.

Utilization of AI for IoT security is particularly extremely encouraging to distinguish any exceptions to typical movement in the framework. With that in mind, we investigate an irregularity based IDS that use the

© 2019 IJSRET

utilization of AI systems, to distinguish any known or obscure assaults on IoT gadgets progressively. We will probably build up a safe, compact, and prepared to-send security framework that gives a viable and compelling answer for verifying future enormous scale IoT systems. In this article, we present an Integrated Intrusion-Detection (IID) framework that works autonomous of IoT conventions and system structure, and requires no earlier information of security dangers.

We build up an artificially smart IDS to give security as a support of IoT systems. We give a diagram of the underlying structure of the proposed framework in our prior research [15]. In this article, we significantly grow the system to consolidate a profound learning calculation to adjust to the changing risk scene and system topology for peculiarity recognition. Our methodology requires no earlier learning of caught arrange payload pairs, traffic marks, or traded off hub address. The proposed IDS classify the system traffic into sessions and examine bizarre qualities of system movement.

1. The Main Contributions Of This Research Are:

Advancement of an inconsistency based interruption location model utilizing profound learning for IoT systems. Execution and assessment of the model for efficiency. The framework of the article is as per the following Section2 discusses the writing survey and the related work. Section3describes the proposed strategy and usage of our IDS, including system observing calculation and peculiarity location calculation, and portrays how the IID dispatches a relief reaction. Section4provides execution subtleties of the IDS created to show a proof of idea. Section5 shows the outcomes for assessment of this framework on ongoing system traffic. Section6presents the end and future work.

2. Exisiting Work

While the IoT has picked up ubiquity, security, protection and unwavering quality difficulties represent a significant boundary to far reaching reception and arrangement of these gadgets [16–19]. The security vulnerabilities presented by heterogeneity and interconnectivity of IoT gadgets and applications makes them an ideal objective for digital offenders to abuse.

The expanding number of assaults and data spills from the IoT has brought about a flood of research tending to security and protection in this space [5][7][20][21]. Regardless of a few preventive measures set up, IoT frameworks keep on being focused by malignant on-screen characters. It has turned out to be more appropriate than any time in recent memory to stress early discovery of interruptions to limit the negative effect on these frameworks. Kasinathan et al. proposed a mark based IDS for 6LoWPAN-based IoT systems [12]. The objective of this framework was to distinguish Dos assaults with a lower false positives rate. This framework was later stretched out to screen bigger systems [22]. Dander et al. proposed a host- based IDS for IoT that likewise relies upon guideline based recognition [23]. The two arrangements depend on mark and guideline based location frameworks that are not equipped for recognizing new and obscure assaults in IoT. These arrangements likewise face the test of habitually refreshing the mark database. Le et al. proposed specification-based IDS, where a human master physically defines the guidelines for every specification, to address RPL assaults, for example, rank-assault, nearby fix assault, and the asset consumption assault. Surendar et al. built up a specification IDS utilizing conduct guidelines to identify sinkhole assaults on 6LoWPAN systems.

The specification-based frameworks examined above are restricted in that they are just as powerful as the aptitude level of the master framework. Erroneous specifications can bring about false discoveries and might imperil the system security. Interruption identification dependent on convention model are created to distinguish abnormalities related with specific IoT conventions. Raza et al. proposed a cross breed mark and inconsistency based IDS, known as SVELTE, for IoT systems dependent on 6LoWPAN convention. This framework is anyway founded on brought together IDS and can't screen traffic between nearby hubs in the system and is specifically focused on just towards recognizing steering convention assaults in IoT.

Bostani et al. proposed a half and half specification IDS for identifying RPL-based convention assaults. The specification-based inconsistency module was utilized to break down the conduct of the host hubs while the irregularity based specialist utilized the solo ideal way woodland calculation for anticipating grouping models. While this strategy introduced promising outcomes, execution of the proposed structure can be improved by consolidating information mining strategies and AI techniques. AI systems have been utilized to improve the viability of interruption identification in conventional systems. With the approach of savvy assaults on IoT, alongside their asset and calculation limitations, it is important to investigate the utilization of AI for verifying IoT frameworks. Liu et al. utilized AI and mark based model to recognize new assaults in I.

This methodology utilizes artificial insusceptible framework for self-adjustment and self-figuring out how to distinguish new assaults. Indeed, even with AI, this methodology still experiences the misfortunes of a mark based location. Krimmling et al. proposed AI for oddity and mark based interruption recognition for verifying IoT systems utilizing the Constrained Application Protocol (CoAP) [13] for vehicle applications. The creators showed utilizing their own assessment structure that the assault location methods bombed when utilized exclusively yet exhibited improved execution when mark

© 2019 IJSRET

and irregularity identification methodologies were joined. Arrington et al. proposed host-based IDS that utilizations AI for irregularity based interruption recognition. The social model proposed in this framework utilizes artificial resistant frameworks that increments in multifaceted nature with the development of IoT organize, inevitably getting to be asset devouring, and corrupting framework execution. Liu et al. built up an ID utilizing stifled fluffy grouping and PCA calculations. This methodology joined AI and information mining strategies and exhibited better location efficiency when contrasted with Bayesian and neural-organize calculations. Be that as it may, with increment in information volume, efficiency and precision of the IDS diminishes.

The creators likewise note that new highlights of IoT will be important to improve their discovery model. It is obvious from the ongoing examination that AI for interruption discovery in the IoT is quickly developing. Notwithstanding, regular AI calculations frequently present low exactness or potentially less versatility for assault discovery on enormous scale IoT systems. In spite of the current research endeavors, AI for oddity location is still in its underlying stages. This article means to advance this examination by specifically exploring profound learning models for interruption discovery in an IoT domain.

3.Intrusion-Detection Framework

To viably distinguish rising digital assaults on the IoT, we build up an autonomous IID framework supported by profound learning calculations. In this area, we talk about the framework engineering and parts of the proposed IDS structure.

II. SYSTEM ARCHITECTURE

Figure1shows the IoT arrange in thought. IoT gadgets in the system are versatile and geologically conveyed inside a range defined by the system and the edge switch goes about as the center or the facilitator. Gadgets convey utilizing remote correspondence conventions, for example, Wi-Fi, Bluetooth BLE, ZigBee, or exclusive correspondence conventions, for example, CoAP or Thread. The proposed IDS is an independent gadget that can be effectively coordinated into the IoT arrange.

The IID works in wanton mode, observing and investigating the system traffic, and utilizations organize virtualization to Interface with switch or other IoT gadgets. Beneath, we briefly plot the various parts of our proposed IDS. More insights concerning the IDS structure and its parts can be found in our previous paper [15]. The components of detection system.

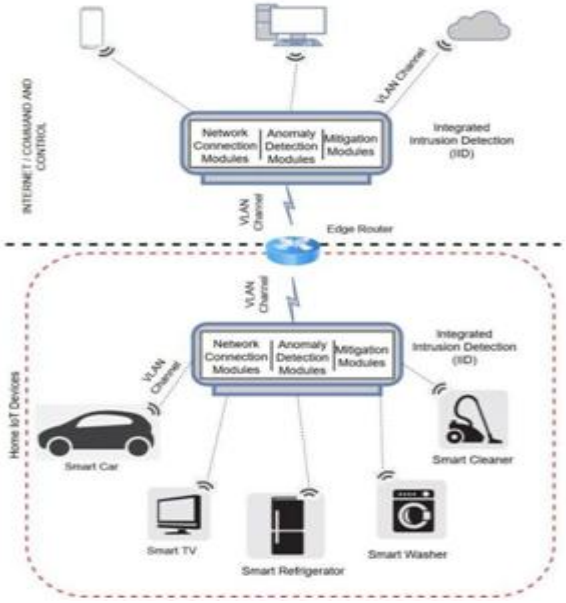

Fig.1. Intrusion Detection System Overview.

The proposed IDS works principally in three stages, specifically the Network Connection Phase, Anomaly-Detection Phase, and the Mitigation Phase as appeared in Figure2.

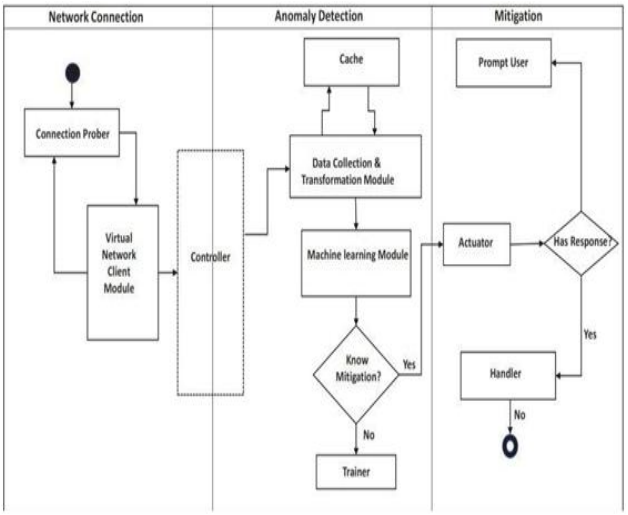

Fig.2. IDS Detection Process.

1. Network Connection Phase

During the Network Connection Phase, the proposed IDS endeavors to decide and send suitable system channel for encouraging interpretation of sniffed arrange traffic. The IDS works in vehicle layer and screens traffic utilizing two modules in this stage, to be specific the association prober module and the virtual system customer module. (I) Connection Prober: The association prober module is in charge of sending test flag and communicates guides to every one of the gadgets inside the host IoT individual

region organize. The module is executed intermittently and on-line, as the correspondence connections are built powerfully inside an IoT organizes. Association Prober module keeps up a rundown of all the dynamic correspondences conventions that are being utilized in the system. It utilizes this rundown to keep up dynamic system interfaces which can be utilized to block distinctive remote correspondence signals, transmitted in the encompassing condition.

Thusly, it endeavors to catch communicate reference points, handshake messages, or session solicitations to become familiar with the correspondence conventions that are being utilized by IoT gadgets. On getting a handshake or a session demand, the association prober module makes an interpretation of the information bundle into fitting system parcel design. Regularly, the association prober module is intended to utilize an optional stockpiling area as a default store area that is all the while reproduced in the physical memory utilizing a reserve handle. In the wake of getting the bit stream, it utilizes the known correspondence conventions to separate the bit stream into various systems bundles and afterward bolsters these parcels into store and the information accumulation and change module (talked about in the following subsection). On the off chance that the association prober falls flat at blocking the communicate guides, or handshake messages,

It endeavors to find the association convention by catching the information bundles transmitted during customary information correspondence of encompassing IoT gadgets. This is made conceivable in light of the fact that CoAP correspondence cycle includes in any event 4 fruitful messages and when association prober neglects to capture a correspondence, it endeavors to accumulate data from progressive messages, bringing about CP's likelihood of achievement, P(S) = 3 4 . The quantity of messages in an IoT correspondence cycle increments as uncovered IoT correspondence is stacked with payload. With increment in number of messages, likelihood of fruitful capture attempt increments, coming about in P(S) > 3 4 , drawing nearer towards solidarity. In most dire outcome imaginable, if CP misses the whole IoT correspondence cycle, the IDS utilizes pre-prepared neural systems to gauge the system conduct in the present time frame. In this way, with further preparing the IDS can be prepared to react to another convention.

2. Detection Using Deep Learning

In this area, we talk about the discovery calculation in detail. Specifically, we utilize profound realizing, which is a subset of AI with expanded flexibility and precision over old style learning calculations. We pick profound learning system, as it beats different arrangements in numerous areas that are exceptionally unstructured and structure heterogeneous examples. They likewise have a favorable position over other AI calculations because of their capacity to steadily take in and extrapolate new includes from a restricted arrangement of preparing information. Moreover, the flimsy and layered structure of consecutive profound neural- organize models makes them the best fit for being sent over a low-fueled and asset compelled compact IoT gadget, as yet encouraging ongoing abnormality recognition. Beneath, we talk about the element extraction, preparing, and the traffic classification utilized in our recognition calculation.

3. Deep -Learning-Based Anomaly Detection

IDSs utilize social classification and reaction to order noxious and kind correspondence. No single message, or highlight on a correspondence cycle can decide the conduct or the idea of the correspondence. Both the subjective and quantitative highlights of a correspondence cycle are required to be seen over some stretch of time to yield its social attributes. We propose the highlights displayed in Table1to describe these subjective and quantitative parts of remote correspondence messages captured by the location module in IoT frameworks.

In an average correspondence cycle between an unmistakable pair of sender and beneficiary hubs, the transmission and gathering rates are relied upon to be comparable. These qualities are anyway unique when the framework is under an assault, for example, refusal of-administration or sinkhole assault. Likewise, transmission-to-gathering proportion is a sensible marker of spoofing and disguising assaults when utilized related to movement term. Transmission mode decides the state and convention of the correspondence.

In view of the pre-prepared conduct, IDS can recognize if the message headers in a correspondence cycle have a known helpless transmission mode, a unintended sender or recipient (through IP addresses), a noxious payload, or these. To order pernicious and generous traffic, the proposed IDS consequently assembles above highlights, for example, transmission-rate, gathering rate, transmission-to-gathering proportion, length, transmission mode, source-IP, goal IP, and the information esteem data from the system traffic. These highlights are chosen with regards to the computational ability, and the handling to execution proportion of compact low-fueled, asset compelled IoT gadgets.

4. Deep-Learning Implementation

We utilize a Deep Belief Network (DBN) to manufacture the feed-forward Deep Neural Network (DNN) as the perceptual learning model. A DBN is a model of un-coordinated associations between various layers, where each layer includes n-number of neural hubs, while a DNN is a kind of feed- forward neural system with numerous layers. Albeit a DNN can be manufactured in various ways, a bit of leeway of building up a DNN model from a DBN model is that the DBN layers can be at first prepared utilizing unaided learning calculation. DNN would thus be able to be made from a model pre-

© 2019 IJSRET

prepared utilizing solo realizing which is quick in contrast with directed learning. We utilize the pre-prepared layers of DBN model to make a DNN model. (Figure3). As appeared in Figure3, the loads for all the concealed layers of this DBN model, signified by we, are gotten by performing solo preparing. In any case, the parameters created from this unaided preparing are utilized for appointing the underlying arrangement of loads. For each system exchange, a parallel classification layer and name data (an) is included at the top layer of the DBN model to effectively build a DNN. Figure4shows that the DBN is increased with parallel classification layer and mark data to change into a DNN. Presently, this DNN model is prepared with a base up directed learning approach utilizing the mark data a. During the regulated learning process, every hub in a DNN layer is allocated with a weight parameter which is controlled by utilizing the angle plummet procedure.

5. Learning Implementation

As referenced before, we utilized Python-based Kara's AI library for the execution of the profound learning calculation. During classification organize, preparing dataset are perused, put away in an information outline and changed over into a grid. Moreover, these datasets are bifurcated into the preparation and testing datasets, where the preparation dataset included 18,989 generous system exchanges and 20,697 malevolent system exchanges, while the testing dataset involved 9494 amiable system exchanges and 10,349 pernicious system exchanges. The framework was at first tried utilizing the marked testing dataset comprising of 19,843 (i.e., 33.333% of info dataset) exchanges, wherein each record establishes of the **6 Qualities; transmission-** rate, gathering rate, transmission-to-gathering proportion, term, transmission mode, source-IP, goal IP, the information esteem data, and the double name data. After the underlying preparing of DNN utilizing marked preparing dataset including 39,686 (i.e., 66.667% of info dataset) exchanges, it was kept running against the testing dataset, with no double name data. Since, the testing dataset had 39,686 of unlabeled records, the profound learning model produces 39,686 forecasts as "0" or "1". We at that point make and instantiate a "Successive" DNN with 3 shrouded layers, and prepare the handling units inside each layer with ReLU initiation work. From that point, the profound learning model is incorporated and fitted with 150 runs, i.e., ages, and the quantity of highlights. At long last, the profound learning model is gathered, and the classifier is allocated and spared in the variable "expectations". Subsequently, in each test, the consequences of the classifier are standardized to a double esteem.

6. Attack Model

We reenact and assess the exhibition of our proposed recognition framework against different assaults on IoT systems, for example, the sinkhole assault, circulated refusal of-administration (DDoS) assault, black hole assault, astute administration assault and wormhole assault. Black hole Attack: In a blackhole assault, the pernicious gadget erroneously publicizes most limited course to goal and afterward quietly drops all parcels on its way making a black hole in the system. Artful Service Attack: In a crafty administration assault, the vindictive gadget expands its trust an incentive by giving exceptionally reliable administrations at first and after that later retreat to giving mediocre support of its own profit.

6.1 Disseminated Denial-of-Service (DDoS) Attack: In a DDoS assault, various traded off IoT gadgets assault an objective server or other system assets bringing about disavowal of administration for clients of the focused on asset.

6.2 Sinkhole Attack: In a sinkhole assault, the pernicious hub may report beneficial course or falsified way to pull in all hubs to divert their bundles through it, going about as a sink.

6.3 Wormhole Attack: In a wormhole passage assault, pair of assailant gadgets plots with one another through a virtual private association. The system parcels gotten by the unfortunate casualty gadget is first sent through the wormhole, and replayed later, coming about in non-upgraded courses.

III. CONCLUSIONS

In this paper, we examined the achievability of conveying AI based interruption location for asset obliged IoT systems. With that in mind, we built up a canny IDS that thoughtfully consolidates organize virtualization and DL calculation to identify atypical conduct on shaky IoT systems. We researched the ideal answer for profound learning-based IDS by assessing the exhibition of our plan against five diverse assault situations, including black hole assault, crafty administration assault, DDoS assault, sinkhole, and wormhole assaults.

Through investigation of accuracy review bends, we got a normal exactness pace of 95% and review pace of 97% for various assault situations. Our analyses additionally exhibit higher F1-scores for all assault situations showing better generally speaking location execution by the proposed framework. In view of the experimentation results acquired from system recreations and test bed executions, we can infer that it is both viable and possible to utilize DL calculations for viable inconsistency identification in the IoT condition. Future work incorporates stretching out the proposed IDS to distinguish different kinds of assaults against the IoT including area ward assaults, for example, cloning of gadget ID, spoofing, and Sybil assaults.

RPL specific misappropriation assaults, disconnection assaults, neighbor assaults and direct assaults can likewise be identified by GPS beacon IDs and approving diary passages, for example, in DODAG (Direction-Oriented Directed Acyclic Graph) table. An increasingly circulated

© 2019 IJSRET

and computationally improved variant of IID might be likewise be utilized towards recognizing zero-day assaults.

REFERENCES

[1]. Gubbi, J.; Buyya, R.; Marusic, S.; Palaniswami,M. Internet of Things (IoT): A vision, architectural elements, and future directions. Future Gener. Comput. Syst. 2013, 29, 1645–1660. [CrossRef]
[2]. Miorandi, D.; Sicari, S.; De Pellegrino, F.; Chlamtac, I. Internet of Things: Vision, applications and research challenges. Ad Hoc Netw. 2012, 10, 1497–1516. [CrossRef]
[3]. Smith, S. IoT Connected Devices to Triple to Over 38Bn Units; Juniper Research: Basingstoke, Hampshire, UK, 2015.
[4]. Roman, R.; Zhou, J.; Lopez, J. On the features and challenges of security and privacy in distributed Internet of Things. Comput. Netw. 2013, 57, 2266–2279. [CrossRef]
[5]. Khan, A. Overview of Security in Internet of Things. In Proceedings of the 3rd International Conference on Recent Trends in Engineering Science and Management, Bundi, Rajasthan, India, 10 April 2016.
[6]. Abomhara, M.; Koien, G.M. Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. J. Cyber Secur. Mobil. 2015, 4, 65–88. [CrossRef]
[7]. Shieh, S.W. Emerging Security Threats and Countermeasures in IoT. In Proceedings of the ACM Asia Conference on Computer and Communications Security, Singapore, 14–17 April 2015.
[8]. Williams, R.; McMahon, E.; Samtani, S.; Patton, M.; Chen, H. Identifying vulnerabilities of consumer Internet of Things (IoT) devices: A scalable approach. In Proceedings of the 2017 IEEE International Conference on Intelligence and Security Informatics (ISI), Beijing, China, 22–24 July 2017; pp. 179–181.
[9]. Hilton, S. Dyn Analysis Summary Of Friday October 21 Attack. Dyn Blog, 26 October 2016.
[10]. Solon, O. Team of hackers take remote control of Tesla Model S from 12 miles away. The Guardian, 20 September 2016.
[11]. Pycroft, L.; Aziz, T.Z. Security of implantable medical devices with wireless connections: The dangers of cyber-attacks. Expert Rev. Med. Devices 2018, 15, 403–406. [CrossRef] [PubMed]
[12]. Kasinathan, P.; Costamagna, G.; Khaleel, H.; Pastrone, C.; Spirito, M.A. DEMO: An IDS Framework for Internet of Things Empowered by 6LoWPAN. In Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security, Berlin, Germany, 4–8 November 2013.
[13]. Krimmling, J.; Peter, S. Integration and Evaluation of Intrusion Detection for CoAP in smart city applications. In Proceedings of the IEEE Conference on Communications and Network Security (CNS), San Francisco, CA, USA, 29–31 October 2014.
[14]. Le, A.; Loo, J.; Lasebae, A.; Aiash, M.; Luo, Y. 6LoWPAN: A study on QoS security threats and countermeasures using intrusion detection system approach. Int. J. Commun. Syst. 2012, 25, 1189–1212. [CrossRef]
[15]. Chawla, S.; Thamilarasu, G. Security As a Service: Real-time Intrusion Detection in Internet of Things. In Proceedings of the Fifth Cyber security Symposium, Cyber Sec ’18, Coeur d’ Alene, ID, USA, 9–11 April 2018; pp. 12:1–12:4.
[16]. Khan, R.; Khan, S.U.; Zaheer, R.; Khan, S. Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges. In Proceedings of the 10th International Conference on Frontiers of Information Technology, Islamabad, India, 17–19 December 2012.
[17]. Xu, T.; Wendt, J.B.; Potkonjak, M. Security of IoT Systems: Design Challenges and Opportunities. In Proceedings of the International Conference on Computer-Aided Design, San Jose, CA, USA, 3–6 November 2014.
[18]. Heer, T.; Garcia-Morchon, O.; Hummen, R.; Keoh, S.L.; Kumar, S.S.; Wehrle, K. Security Challenges in the IP-based Internet of Things. Wirel. Person. Commun. 2011, 61, 527–542. [CrossRef]
[19]. Sfar, A.R.; Natalizio, E.; Challal, Y.; Chtourou,
[20]. Z. A roadmap for security challenges in the Internet of Things. Digit. Commun. Netw. 2018, 4, 118–137. [CrossRef]
[21]. Zhou, W.; Jia, Y.; Peng, A.; Zhang, Y.; Liu, P. The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved. IEEE Internet Things J. 2018. [CrossRef]
[22]. Zhao, K.; Ge, L. A Survey on the Internet of Things Security. In Proceedings of the 2013 9th International Conference on Computational Intelligence and Security (CIS), Leshan, Sichuan, China, 14–15 December 2013.
[23]. Kasinathan, P.; Pastrone, C.; Spirito, M.A.; Vinkovits, M. Denial-of-Service detection in 6LoWPAN based Internet of Things. In Proceedings of the 2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Lyon, France, 7–9 October 2013; pp. 600–607.
[24]. Danda, J.M.R.; Hota, C. Attack Identification Framework for IoT Devices. In Information Systems Design and Intelligent Applications; Springer India: New Delhi, India, 2016; pp. 505–513.
[25]. Le, A.; Loo, J.; Chai, K.K.; Aiash, M. Specification-Based IDS for Detecting Attacks on RPL-Based Network Topology. Information 2016, 7, 25. [CrossRef]

© 2019 IJSRET

[26]. Surendar, M.; Umamakeswari, A. InDReS: An Intrusion Detection and response system for Internet of Things with 6LoWPAN. In Proceedings of the 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, India, 23–25 March 2016.

© 2019 IJSRET