IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Analysis of Security System for IoT Environment

1.P. Archana, Assistant. Professor, Sreyas Institute of Engineering and Technology

2.P.VijayaLakshmi, Assistant. Professor, Sreyas Institute of Engineering and Technology

Abstract

These days, the Internet of Things (IoT) network, is progressively turning into an omnipresent availability between various progressed applications, for example, keen urban areas, shrewd homes, savvy frameworks, and numerous others. The arising organization of brilliant gadgets and articles empowers individuals to settle on keen choices through machine to machine (M2M) correspondence. Most true security and IoT-related difficulties are defenseless against different assaults that represent various security and protection challenges. Accordingly, IoT offers productive and successful arrangements. interruption location framework (IDS) is an answer for address security and protection challenges with recognizing diverse IoT assaults. To build up an assault recognition and a steady organization, this present paper's principle objective is to give an exhaustive diagram of existing interruption location framework for IoT climate, network protection dangers challenges, and straightforward issues and concerns are broke down and talked about. In this paper, we propose programming characterized IDS based dispersed cloud design, that gives a protected IoT climate. Experi-mental assessment of proposed engineering shows that it has preferable recognition and exactness over conventional techniques.

1. Introduction

The data innovation age, Internet of Things (IoT) is known as the most energizing advancements. The web permits associated gadgets to develop dramatically consistently, and it has been declared that more than 50 million gadgets will be associated through the web by 2020 [1]. The IoT innovation's motivation is to interconnect all articles so as to make all PCs, programmable, canny, and make it safer to speak with people. Sensors and organizations permit everything to speak with one another straightforwardly for trading basic data. It is conceivable by machine to machine (M2M) correspondence later on. Various viable of IoT applications can be utilized practically in numerous fields, for example, keen city applications (savvy home, and shrewd network, medical care, and others), where those applications improve the personal satisfaction [2]. The idea of the interruption identification framework (IDS) expects to identify a danger or interruption into the organization, and it effectively tracks the organization by recognizing likely occasions and logging data about them by halting occurrences. Interruption discovery and anticipation framework (IDPS) which is a mix of two frameworks used to screen occasions happening in an organize and assess them for potential infringement or episodes in security strategies and furthermore the way toward performing interruption recognition and stop to distinguish occurrences.

Utilizing the IoT framework in numerous applications areas, for example, medical care, keen home, shrewd industry, natural observing, and others gives huge advantages to the IoT framework. IoT security issues are a huge concern, which is classification, uprightness, accessibility, and approval [3,4]. The joining of true items with IoT, notwithstanding, acquires a scope of online protection dangers day by day exercises. Those potential assaults happen against basic framework in IoT, for example, refusal of administration (DoS), man-in-the-center (MITM), and others [5]. They can bargain any gadget, the principle worker, if it's undermined by the assailant, the entire framework to close down. To tackle these issues, IDS perceived as one of the key devices assumes an essential function in the IoT security structure utilized for data frameworks and customary organizations. It distinguishes many known and obscure assaults not exclusively to identify known assaults.

In this investigation, we give brief diagram research identified with IDS for IoT security issues. Our examination objective exhibits best in class from an alternate point of view, which incorporates the engineering of the layered IoT climate and security system. We likewise center around future suggestions and direction identified with network safety issues in the IoT climate. Considering the advancement of IDS for the IoT climate presents critical difficulties for security. Subsequently, the investigation of our overview offers some vital commitments as follows:

- First, we sketch pertinent parts of security issues, weaknesses, and assault surfaces on the IoT climate.

- Second a far reaching conversation on open issues in IDS for IoT climate.

- Finally, assess the proposed engineering and shows that it is superior to customary strategies.

The rest of our examination organized as follows: The writing audit and related work are summed up in Section 2. Segment 3 gives a review of the IoT security climate; Section 4 portrays issues and difficulties identifying with IoT security. Exploratory outcomes and examination are appeared in Section 5. At last, Section 6 closes our work.

2. Related Work

While IoT has been picking up fame, security and protection challenges present huge hindrances for organization of these jumps and far and wide selection. Interruption location has been a significant field of work for over thirty years. Information in organization interruption identification, alongside security needs, has expanded among scientists. Numerous analysts have examined and talked about the open-finished exploration issues of the IDS for the IoT climate, as it's appeared in Fig. 1.

Discovery Methods for Intrusion Detection System

In the IoT climate, the arrangement of IDS can't succeed indicated security issues. The IDS endeavor to follow either the gadget or the organization occasions of conceivably pernicious assaults over the organization [6,7]. The greater part of the examination work dependent on interruption identification and avoidance framework zeroed in on distributed computing [8,9]. IDS's motivation is to recognize unapproved access from aggressors. These frameworks are considered to include: remote neighborhood (WLAN), mists, wide territory organization (WANs), and others [10]. In view of Jun and Chi [11] referenced that powerful IDS should be basic and precisely identified for various security dangers in the IoT climate. As per the organization of IoT based IDS appeared in Fig. 1, it very well may be ordered into irregularity based IDS, have based IDS, an organization based IDS, and dispersed IDS.

Anomaly based IDS (AIDS): For the situation of AIDS, known as unique conduct based discovery, it makes critical bogus cautions and creates alarms, where obscure dangers can be recognized at different levels and weaknesses can be distinguished [12,13], and assessed the fitting moves to make. Then again, IDS keep on demonstrating a generally high pace of bogus positive [14]. Inconsistency remembers gathering information for approved clients' activities over a period to follow gadget activity and to distinguish either ordinary or deformity. These groupings depend on guidelines, as opposed to marks, endeavoring to identify any assault in ordinary activity.

- Host-based IDS (HIDS): The HIDS is programming introduced have PC of the organization ability to screen, dissect, and gather traffic exercises on the organization interfaces that are started from the host of framework application. IDS have restricted perspectives, and it can just recognize malignant practices for a solitary host.

- Network-based IDS (NIDS): The NIDS makes peculiarity identification and mark recognition. For instance, in Signature identification, list the sorts of assaults appropriate for it, for example, application layer surveillance, strategy approval, transport layer observation, and organization layer recon-naissance. The organization based interruption identification framework works by checking the traffic as the organization streams over the organization foundation. Both NIDS and HDIS have abilities for distinguishing and checking malevolent exercises [15].

- Distributed IDS (DIDS): It comprises of various IDS on a broad organization, where all of which imparts and encourages progressed network observing, moment assault information, and episode investigation. It joins data from the quantity of sensors, including both organization and hose-based IDS. The focal analyzer is best prepared to distinguish and react to interruption exercises.

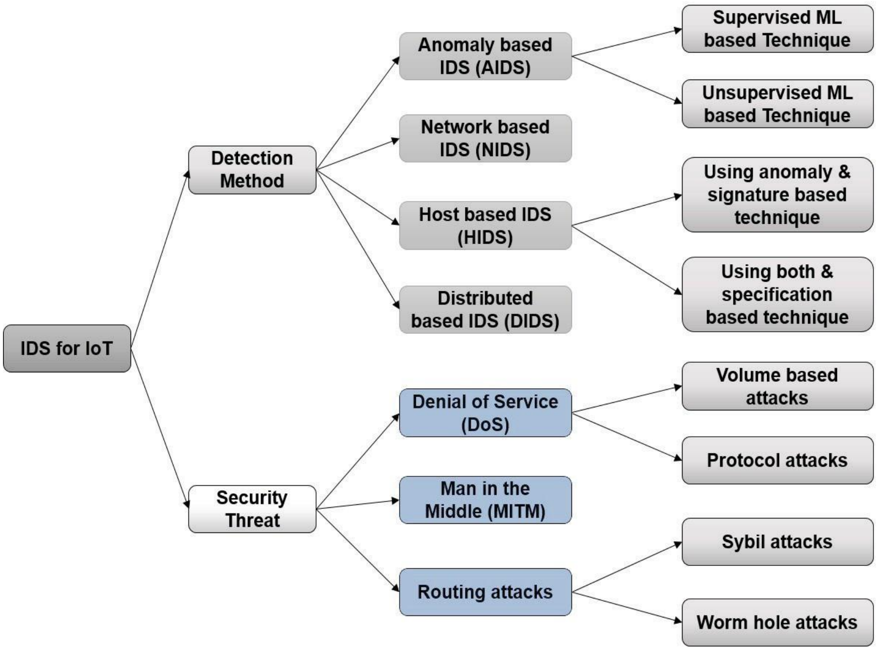

Fig. 1. Intrusion Detection System IDS for IoT.

Security Threats

The IoT security dangers are defenseless against different assaults, in light of other examination makes reference to various sorts of assaults that have been talked about in the IDS for IoT proposition. Therefore, empowering IoT arrangements will incorporate different frameworks, offices, and norms, each with its security and protection rules. In light of three parts of trading information among clients and articles: (1) restricted force for the IoT climate,

(2)a huge number of interconnected gadgets have noticed that regular insurance, and (3) security can't be applied straightforwardly to such IoT innovations, some sign of how IoT gadgets are helpless to assault has been recognized [16,17].

As per Kollias et al. [18] referenced the IoT innovations had been built up that could leave weaknesses assaults identified with security and protection issues in the IoT network. Some other examination contemplates dependent on security dangers that can influence substances in IoT is coordinated as the accompanying classes appeared in Fig. 1: directing assaults, MITM, DoS, listening in assaults [19].

Existing Research Studies

Lately numerous creators have been reviewed pertinent to IoT and will in general zero in on specific parts of IDS. A review dependent on AI methods which zeroing in on IDS for the remote sensor organization (WSN) and IoT [20]. Kasinathan et al. [21] proposed an organization based DoS discovery for interruption identification framework engineering, where utilizing the IDS test way to deal with screen 6LoWPAN traffic. In view of Buczak and Guven [22] study makes reference to IDS on the overall framework routinely utilized for explicit WSN and IoT, and features a specific number of issues with strategies specifically for the intricacy of those which require securing. Abudaliyev et al. [23] notice a review related on the qualities of IDS in WSN, where the weaknesses for approval incorporates a low measure of information accessible, absence of widespread assault recognition and helpless energy utilization. Another comparable review that centers around IDS for WSN presented [24]. In Table 1, we just referenced a similar outline review on IDS for IoT security.

Table 1. Overview of IDS for IoT environment

	[25]	[26]	[27]	[28]	[29]	[30]	[31]	[32]	[33]	Our work
Architecture										
Centralized	3	3	3	3	✓	✓	3	3	✓	✓
Distributed	✓	✓	3	3	3	3	3	3	✓	✓
Hybrid	3	3	3	3	3	3	✓	✓	✓	3
Hierarchical	3	3	✓	✓	3	3	3	3	3	3
Detection technique										
Anomaly	✓	3	3	✓	✓	✓	✓	3	3	✓
Hybrid	3	✓		3	3	3	3	3	3	3
Signature	3	3	3	3	3	3	3	3	3	3
Specification	3	3	3	3	3	3	3	✓	3	3
Machine learning	3	3	3	3	✓	✓	3	✓	✓	✓
Types										
Network-based IDS	✓	✓	✓	✓	3	✓	✓	✓	✓	✓
Host-based IDS	3	3	3	3	✓	3		3	3	✓
Technology focus										
Routing protocol for wireless	3	3	3	3	3	3	✓	✓	✓	✓
Wireless sensor network	✓	✓	✓	✓	3	3	3	3	✓	✓
Mobile devices	3	3	3	3	✓	3		3	✓	✓

3. IoT Security

In this part, is investigated a diagram of current security issues inside the IoT climate. IoT is known as the new age of the web; it comprises of countless impromptu associated gadgets, and highlights profoundly limit these gadgets. The IoT engineering centers around the center of three layers, as appeared in Fig. 2.

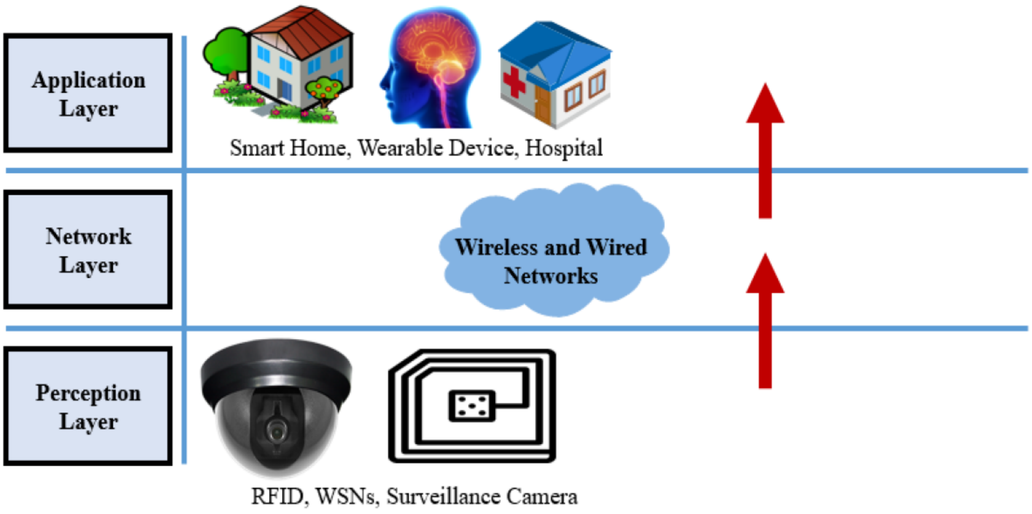
Application Layer
Smart Home, Wearable Device, Hospital
Network Layer
Wireless and Wired Networks
Perception Layer
RFID, WSNs, Surveillance Camera

Fig. 2. IoT Architecture and attacks.

IoT Layer Architecture

Perception layer, beginning from this layer is the most minimal level and information entryway for IoT, where correspondences happen among hubs and gadgets, it's basic to have safety efforts guarding against any break. The observation layer segments are M2M, radio-recurrence ID (RFID), and sensor network [34]. To start with, the M2M considered as one of the significant components of the IoT, which empowers interconnection and interoperability between machines over the organization [35]. Second, RFID permits the item to remotely convey various kinds of correspondence over the IoT climate, prompting the capacity to screen information. The last sensor organization, is con-sidered significant data in the recognition layer and is another element that takes care of the sign information base.

- The network layer structures one of the biggest and is liable for empowering IoT gadgets to com-municate with different gadgets also with the application administrations [36]. The organization layer comprises of an organization interface, Wi-Fi, Ethernet, cell, Zigbee, wise administration, RIFD, and different gadgets. Organization highlights are utilized for preparing and send sensor information [37]. These sensors are little, with limit figuring force and restricted handling.

- Application layer incorporates an IoT framework comprising of an organization, for example, a cloud framework for information stockpiling and actuators. It is liable for sorting out the information got and communicated to another IoT layer. The IoT application layer strategy, channels and ordinarily comprises of those related, regularly situated by going a message through all regions of the organization from the observation layer [38]. Application is relied upon to introduce high-security necessities, however it presents normal security issues, for example, identified with information trustworthiness, dependability, and security assurance. In this manner, the security of IoT should be tended to.

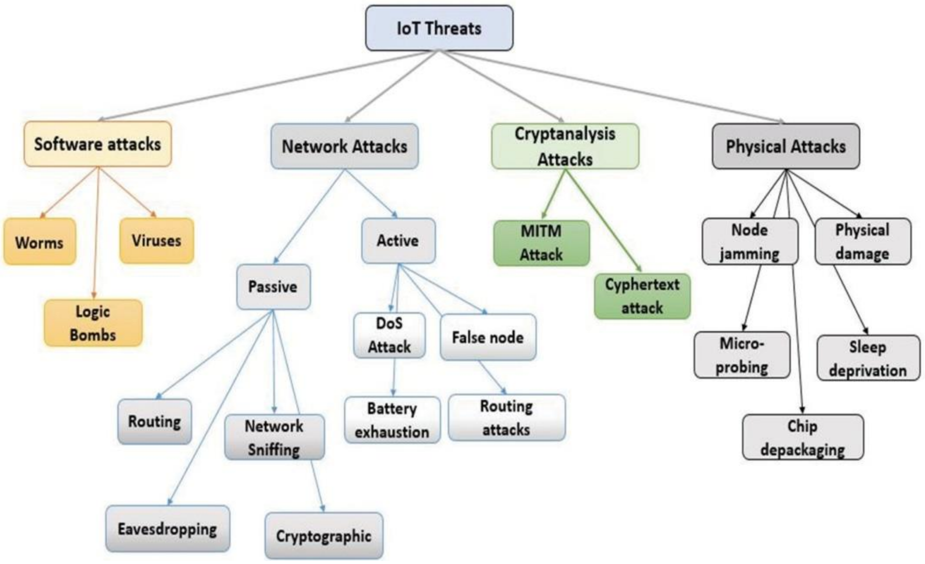

Fig. 3. Detailed taxonomy of threats in IoT.

IoT Cyber-Attacks

In network safety, privacy, respectability, and accessibility are notable. Various kinds of assaults are uncovered in the IoT network either from inward or outer, Fig. 3 portrays point by point scientific classification of dangers in IoT, where these sorts of assaults are for the most part delegated two sorts as outside and inside assaults. The external assault is viewed as when the aggressor isn't important for the organization, while in an inside assault, malignant hubs are essential for the organization, along these lines we talk about some digital assaults in the IoT climate.

- Software assaults: It is the essential wellspring of security weakness and it comprises of different sorts of assaults in IoT, these assaults can repeat without human activity and it misuses the framework by utilizing rationale bombs, infections, worms and different instances of programming assaults that intentionally infuse framework code through its correspondence interface which can take data and even harm gadgets on IoT framework [39-41].

- Network assaults: It focused on the IoT climate, comprises of two unique sorts of assaults, uninvolved and dynamic, that may influence the IoT framework climate. Detached assaults which are under gatecrashers screen a framework is performed by a few assaults permitting the aggressor to gather data from the sensor, moreover, by listen in, an assailant could keep an eye on a correspondence channel causing protection infringement (e.g., side chain, cryptographic, snooping, directing) [42,43]. The dynamic assault includes the utilization of data gathered during the inactive assault to bargain the organization, and the aggressor alters the IoT framework to change the arrangements. Attempt to break the assurance highlight of information associated with the locale or wreck the organization correspondence framework. Assaults may incorporate a grouping of drug, disturbance, and numerous kinds of assaults (e.g., directing assault, DoS, bogus hub, and battery depletion).

- Cryptanalysis assaults: This kind of assault is a sort of decoding and investigation of codes scrambled and cyphertext where they utilize some arithmetic equations for search weaknesses and nose into cryptography calculations, and their motivation is to discover encryption key used to breaking encryption. These kinds of assaults are referred to just as usage assaults, and it incorporates (MITM assault, picked ciphertext assault) [44].

- Physical Attacks: Physical assaults know as a basic kind of cryptanalysis used to find shrouded parts of gadgets, and to recognize IoT weaknesses zeroed in on the equipment segment, the assailant will attempt to get actual access before an assault is finished by making a bogus assault test. It uncovered weaknesses, for example, (e.g., miniature examining, hub sticking, actual harm chip Re-bundling, and lack of sleep), making harm the sensor hub. The foes change the conduct of gadgets that includes the IoT climate framework [45].

4. Proposed Distributed Cloud Architecture

In this segment, we portray the plan outline of proposed appropriated cloud engineering, and investigation results and examination.

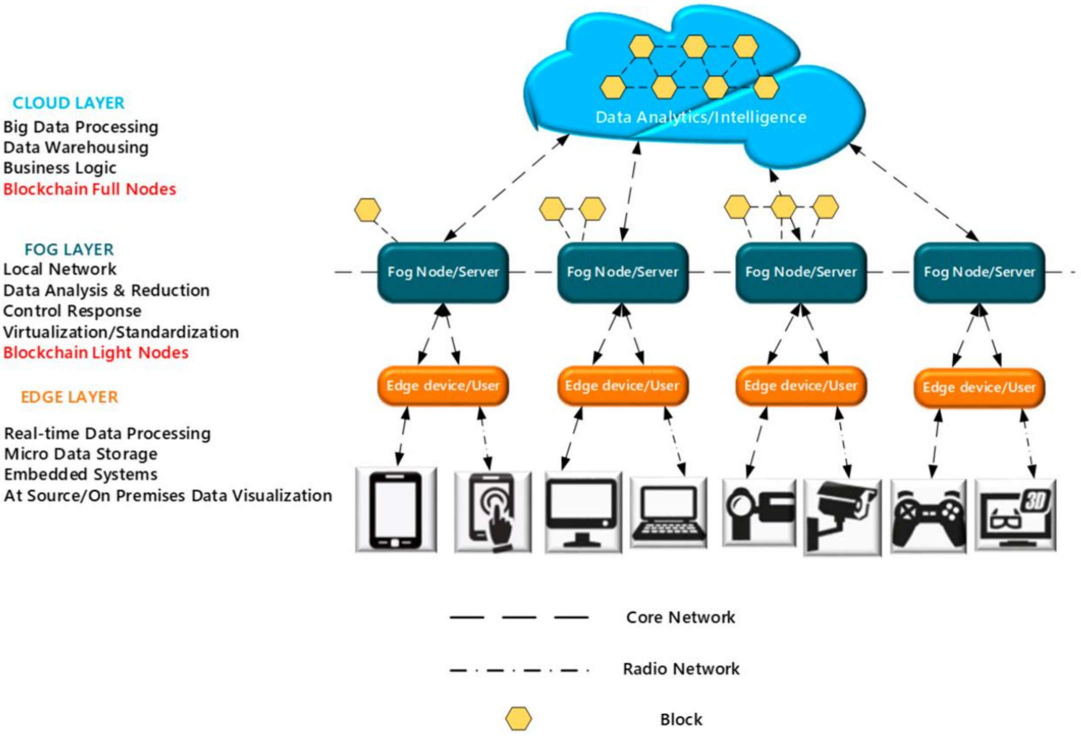

Fig. 4. Software-defined IDS based distributed cloud architecture.

Design Overview of ProposedArchitecture

We talked about the central security concerns and some wellbeing estimates identified with the IoT archi-tecture alluded to in Section 3. To make sure about the IoT framework inside, it is considered as four layers. In Fig. 4 presents our proposed strategy, we will survey inside and out and security highlights of each level in detail.

In view of Patel et al. [46] research proposes the possibility of another Open Flow switch that includes IDS in it, making Open Flow convention more secure. The other creator proposed a structure with the programmability benefits gave by SDN to incorporate the IDS engineering to distinguish dubious bundles [47]. The creators present the definition in [48] to distinguish criminal operations did in the SDN setting. We propose utilizing SDN advances and AI calculations to follow and distinguish noxious exercises in the SDN information plane. We increment the exhibition and accomplish the recognizable proof of U2R assaults.

Our proposed programming characterized IDS for dispersed cloud design determination comprises of the accompanying four parts in various layers of the IoT climate: the principal layer of discernment comprising of IoT modules, second SDN-empowered switch, third group SDN regulator and last SDN regulator.

•IoT gadgets in the recognition layer, end-clients on other IoT gadgets ought to have their commitments. These IoT gadgets which are an assortment of interconnected registering gadgets, mechanical, advanced machines, reconnaissance cameras, keen gadgets, wearable gadgets, and different gadgets that are connected to a SDN switch with one of a kind identifiers and the capacity to move information over an organization without the requirement for human-to-human or PC to-PC communication.

•SDN-empowered switch in edge layer, in this framework, each end client is accepted to have a switch that is viable with SDN and supports open stream convention. The change expands on security approaches and rules. The switch is the endpoint of a specialist organization. SDN permits changing to arrange specialist organizations utilizing a cross breed approach.

•IDS regulator in mist layer, the end-clients utilizing in IDS regulator which has the accompanying key part. (1) Sensors ready to gather information, for instance, bundles utilizing TCP-dump or Wireshark, log documents (for applications), framework call follows (for the working framework). (2) Analyzer, the information acquired is gotten, assessed, and chose whether it is encroached. Furthermore, (3) UI empowers IDS execution and control activities to be deciphered by security specialists, framework chairmen, and different clients.

•SDN regulator in the cloud layer, SDN regulator stays with the media transmission specialist co-op at the most significant level inside the Soft Things framework. This SDN regulator deals with all regulators in the IoT climate. This regulator has an extensive review of traffic stream and various occasions on the organization.

AI strategies have been utilized in regular organizations to improve SDN execution to dodge and forestall numerous IoT assaults. With insightful assaults on the IoT structure layers, its assets, and computational limitations, it is critical to investigate the utilization of AI methods to ensure the IoT network and to recognize irregularities against typical parcels. It is perceived that these days, notwithstanding, AI is developing quickly for SDN and IDS. For the edge and mist layer, which are handling, network gadgets limit and capacity, as mist layer have not to figure it out. By the by, we recommend utilizing a conveyed, stable SDN regulator network dependent on the IDS for the edge and haze layer to be virtual machines associated go to the handling and capacity unit seen as an alternate substance. Its utilization SDN for the empowered disseminated cloud ought work the organization as well as track and adequately safeguard the organization from outside and inward assaults.

Experiment and Analysis

In this subsection, we run our analysis over the NLS KDD ace dataset utilizing and led on Ubuntu 18.10, with 6 GB of RAM and 100 GB of hard drive space on VMware. To prepare and test our Machine learning model, we use Weka (3.9.3) and TensorFlow, and for SDN, SDN emulator, and Maxi-Net.

Evaluation

The exhibition investigation of our work approach normally acted regarding exactness, review, and precision. Programming characterized IDS requires low bogus caution high productivity and high location rate. The disarray lattice is utilized to gauge those boundaries; hence, the assessment results are the accompanying.

- Precision shows the number of interruptions are anticipated by and IDS. The higher the P, the lower caution. The extent of right sure order for all certain grouping.

P = TP TP+FN

Accuracy: Accuracy shows the stream shows precisely sorted around the whole traffic follows. The extent of arrangements, over all N cases, they were right.

Acc =TP+TN /TP+TN+FP+FN (2)

- Recall shows the rate number of expected interruptions versus any genuine interruption, its high R-esteem required. The extent of positive models which have been accurately arranged.

R= TP /TP+FN (3)

Graphical and tabular analysis

Precision was utilized for correlation since it ascertains the proportion of effectively recognized cases to the absolute number of occurrences. As appeared in Fig. 5, obviously appropriated haze arrangement regarding exactness, discovery rate, review in six separate assault situations. The proposed engineering is marginally lower regarding recognition rate in light of the fact that the gadget to share data to join and settle on the most precise choi

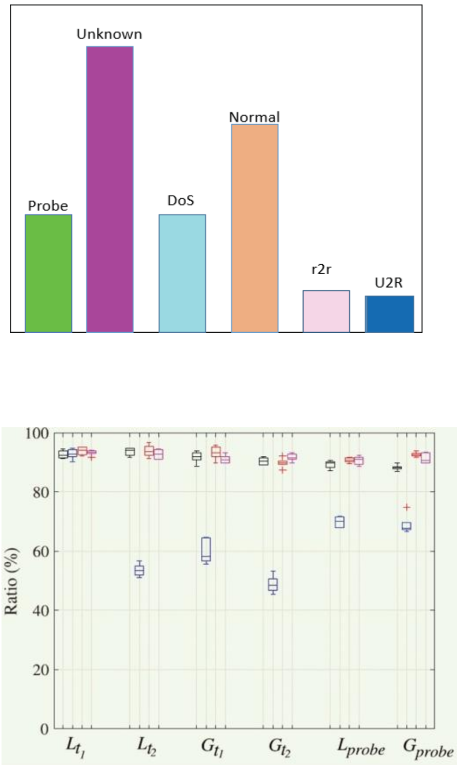

Fig. 5. Anomaly detection performance with accuracy: (a) accuracy and (b) different attack types predicted.

The exhibition of the proposed design utilizing the NLS KDD ace dataset was assessed the mix of our picked calculations comparative with a few classes of standard element choice and AI calculations show in Table 2.

In light of the examination and trial assessment, we can say that proposed design is helpful for assault recognition, indicating that it offers preferable identification and exactness over conventional techniques.

TP rate	FT rate	Precision	Recall	MCC	RDC area	PRC area	Class
0.974	0.012	1.883	0.926	0.920	0.997	0.967	U2R
0.600	0.001	0.999	0.600	0.614	0.999	0.999	R2L
0.095	0.007	1.147	0.095	0.109	0.966	0.261	Probe
0.976	0.000	1.000	0.976	0.840	0.966	0.995	DoS
0.897	0.005	0.792	0.897	0.965	0.994	0.873	Normal
0.953	0.000	0.976	0.953	0.012	0.985	0.762	Unknown

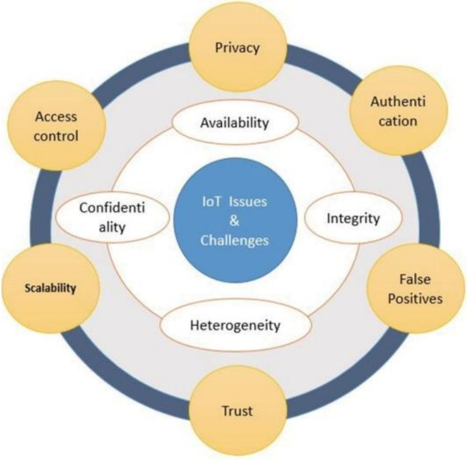

Fig. 6. IoT Issues and challenges.

5. IoT Security Issues

An incredible potential is given by the IoT, where one of the fundamental destinations is to change the manner in which we perform various exercises and way of life of individuals in the new world. Remote correspondence frameworks have been inclined to security weaknesses from the very initiation; in this manner, it is vital to feature the security issues for IoT identified with security and protection that can be summed up dependent on Fig. 6 as privacy, accessibility, versatility, uprightness, and heterogeneity.

•Confidentiality expresses that trust is a central issue for IoT clients sharing data by things and permits not to be undermined by an assailant. At the point when an aggressor can without much of a stretch catch messages that pass from the sender-collector so the protection can be changed and spilled. Consequently, it's necessary a protected directive for the IoT climate [49,50].

•Availability, as we come to depend on IoT security inside our day by day lives, it should think about the accessibility of IoT framework, this potential for interruption because of network gadgets disappointment, emerging assaults, for example, DoS, DDoS, sticking assaults, which is considered as in excess of a bother, subsequently the effect of absence of accessibility could mean a misfortune [51].

•Integrity, guaranteeing the uprightness information in an IoT network it's considered as another issue for security, because of the progression of enormous information created by countless associated gadgets, it should ensures that message has not to be modified by an assailant or unapproved client while in transmission over the organization to protecting the respectability of IoT [52]. Endeavors have been made to guarantee information trustworthiness [53,54]. In not so distant future information respectability in IoT should get extensive consideration.

•Heterogeneity, known as a variety of various equipment execution over the IoT organization, for example, a memory impression, calculation power, conventions, and so forth, assaults that happen on privacy, accessibility, and trustworthiness, because of the IoT security heterogeneity issues to forestall sorts of assaults are too intricate, the nonappearance of basic security administration is the most concerning issue

Challenges

•Attack model: This model for IoT, since a few savvy gadgets are interconnected. Subsequently, digital aggressors can direct progressed and convoluted assaults. Along these lines, it is important to find more reasonable assault models and discover a harmony between discovery rate and asset devoured.

•Secure ready traffic: The assurance of IDS correspondence channels is another steady concern challenge for the IoT framework. An assortment of organizations assume control over control to make sure about correspondence between IDS segments and hubs across the organization. As an outcome, in the IoT case, numerous challenges in making sure about the IDS and helpless insurance strategies are utilized to make sure about correspondence among hubs and sensors, so that permits the assailant to effectively screen and unscramble network traffic. The significance needs of assurance with a solid IDS correspondence framework for IoT.

•Trust: It is based on the reason that nothing will influence the ideal person. As an outcome, notwithstanding the IoT program, numerous heterogeneous organizations can be undermined by being connected through the Internet. This association with different frameworks brings settle for less that can produce trust difficulties. The trust framework should meet and be refreshed with the development of IoT gadgets [59]. Despite the fact that few specialists have been proposed to assess positive standing and cooperation, it's necessary further examination.

•Malicious code assaults another test, which happens different assaults in IoT that target application projects, for example, DoS, worms, it intends to assault surveillance cameras, switches. These kinds of assaults can abuse the presence of programming weaknesses. A typical assault component is an arising registering framework, for example, IoT security, a recognition system for IoT which centers around singular identification dangers.

•Privacy: It required extraordinary contemplations for IoT to forestall client's data over the organization [60]. Guaranteeing protection in the IoT climate is considered as a test for setting up secure correspondence tending to related information. Protection hazard emerges as the article in the IoT gather, which total pieces of information.

	DoS	Eavesdrop	Routing	Phishing	Malicious code
Application layer	3	3	3	✓	3
Network layer	✓	3	✓	3	✓
Perception layer	3	✓	3	3	✓

6. Conclusions

Today, it is accepted that the quantity of IoT gadgets being associated overall will in general develop on everyday schedule; its application includes numerous activities. In this paper, we have distinguished assaults on IoT gadgets for which the quantity of recorded occasions of noxious assaults keeps on expanding; data security specialists and analysts routinely discover weaknesses utilized by cybercriminals that could bargain protection, security, and assurance of buyers. Subsequently, the recurrence and assortment of security dangers to these frameworks have expanded severally, showing the estimation of a successful interruption detection framework. Accordingly, to sum up this paper, we introduced an exhaustive study about programming characterized based IDS for IoT security climate, we gave a nitty gritty examination about every innovation in an alternate section, and we contemplated the IoT security dangers and the assembly. Test assessment of proposed design shows that it has preferable recognition and exactness over conventional strategies. Our future work intends to create and execute a more solid and secure SD-IDS innovation for the IoT climate.

References

[1] S. C. Mukhopadhyay and N. K. Suryadevara, "Internet of things: challenges and opportunities," in *Internet of Things: Challenges and Opportunities*. Cham, Switzerland: Springer International Publishing, 2014, pp. 1-17.

[2] O. Vermesan and P. Friess, *Internet of Things-from Research and Innovation to Market Deployment*. Aalborg, Denmark: River Publishers, 2014.

[3] S. P. Anilbhai and C. Parekh, "Intrusion Detection and Prevention System for IoT," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, vol. 2, no. 6, pp. 771- 776, 2017.

[4] S. Tanwar, S. Tyagi, and S. Kumar, "The role of internet of things and smart grid for the development of a smart city," in *Intelligent Communication and Computational Technologies.* Singapore: Springer, Singapore, 2018, pp. 23-33.

[5] M. Anirudh, S. A. Thileeban, and D. J. Nallathambi, "Use of honeypots for mitigating DoS attacks targeted on IoT networks," in *Proceedings of 2017 International Conference on Computer, Communication and Signal Processing (ICCCSP)*, Chennai, India, 2017, pp. 1-4.

[6] A. Mehmood, M. Mukherjee, S. H. Ahmed, H. Song, and K. M. Malik, "NBC-MAIDS: Naive Bayesian classification technique in multi-agent system-enriched IDS for securing IoT against DDoS attacks," *The Journal of Supercomputing*, vol. 74, no. 10, pp. 5156-5170, 2018.

[7] R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, Fog et al.: a survey and analysis of security threats and challenges," *Future Generation Computer Systems*, vol. 78, pp. 680-698, 2018.

[8] S. G. Kene and D. P. Theng, "A review on intrusion detection techniques for cloud computing and security challenges," in *Proceedings of 2015 2nd International Conference on Electronics and Communication Systems (ICECS)*, Coimbatore, India, 2015, pp. 227-232.

[9] A. A. Gendreau and M. Moorman, "Survey of intrusion detection systems towards an end to end secure internet of things," in *Proceedings of 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)*, Vienna, Austria, 2016, pp. 84-90.

[10] C. Jun and C. Chi, "Design of complex event-processing IDS in internet of things," in *Proceedings of 2014 Sixth International Conference on Measuring Technology and Mechatronics Automation*, Zhangjiajie, China, 2014, pp. 226-229.

[11] A. Patel, Q. Qassim, Z. Shukor, J. Nogueira, J. Junior, and C. Wills, "Autonomic agent-based self-managed intrusion detection and prevention system," in *Proceedings of the South African Information Security Multi- Conference (SAISMC 2010)*, Port Elizabeth, South Africa, 2011, pp. 223-234.

[12] J. H. Lee, M. W. Park, J. H. Eom, and T. M. Chung, "Multi-level Intrusion Detection System and log management in Cloud Computing," in *Proceedings of 13th International Conference on Advanced Communication Technology (ICACT2011)*, Seoul, Korea, 2011, pp. 552-555.

[13] M. F. Elrawy, A. I. Awad, and H. F. A. Hamed, "Intrusion detection systems for IoT-based smart environments: a survey," *Journal of Cloud Computing*, vol. 7, article no. 21, 2018.

[14] P. S. Kenkre, A. Pai, and L. Colaco, "Real-time intrusion detection and prevention system," in *Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA)*. Cham: Springer, 2014, pp. 405-411.

[15] B. B. Zarpelao, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, "A survey of intrusion detection in Internet of Things," *Journal of Network and Computer Applications*, vol. 84, pp. 25-37, 2017.

[16] S. Notra, M. Siddiqi, H. Habibi Gharakheili, V. Sivaraman, and R. Boreli, "An experimental study of security and privacy risks with emerging household appliances," in *Proceedings of 2014 IEEE Conference on Communications and Network Security*, San Francisco, CA, 2014, pp. 79-84.

[17] C. Kolias, A. Stavrou, J. Voas, I. Bojanova, and R. Kuhn, "Learning Internet-of-Things security 'Hands-On',"
IEEE Security & Privacy, vol. 14, no. 1, pp. 37-46, 2016.

[18] O. Garcia-Morchon, S. Kumar, S. Keoh, R. Hummen, and R. Struik, "Security considerations in the IP-based Internet of Things: draft-garcia-core-security-06," Internet-Draft, Internet Engineering Task Force, 2013.

[19] E. Benkhelifa, T. Welsh, and W. Hamouda, "A critical review of practices and challenges in intrusion detection systems for IoT: toward universal and resilient systems," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3496-3509, 2018.

[20] P. Kasinathan, C. Pastrone, M. A. Spirito, and M. Vinkovits, "Denial-of-service detection in 6LoWPAN based Internet of Things," in *Proceedings of 2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, Lyon, France, 2013, pp. 600-607.

[21] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153-1176, 2016.

[22] A. Abduvaliyev, A. K. Pathan, J. Zhou, R. Roman, and W. Wong, "On the vital areas of intrusion detection systems in wireless sensor networks," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 3, pp. 1223- 1237, 2013.

[23] A. Gupta, O. J. Pandey, M. Shukla, A. Dadhich, S. Mathur, and A. Ingle, "Computational intelligence based intrusion detection systems for wireless communication and pervasive computing networks," in

[24] H. A. Arolkar, S. P. Sheth, and V. P. Tamhane, "Ant colony based approach for intrusion detection on cluster heads in WSN," in *Proceedings of the 2011 International Conference on Communication, Computing & Security*, Rourkela, India, 2011, pp. 523-526.

[25] D. Shreenivas, S. Raza, and T. Voigt, "Intrusion detection in the RPL-connected 6LoWPAN networks," in *Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security*, Abu Dhabi, United Arab Emirates, 2017, pp. 31-38.

[26] T. Jiang, G. Wang, and H. Yu, "A dynamic intrusion detection scheme for cluster-based wireless sensor networks," in *World Automation Congress 2012*, Puerto Vallarta, Mexico, 2012, pp. 259-261.

[27] G. Padmavathi and D. Shanmugapriya, "A survey of attacks, security mechanisms and challenges in wireless sensor networks," *International Journal of Computer Science and Information Security*, vol. 4, no. 1 & 2, pp. 1-9, 2009.

[28] A. Milenkoski, M. Vieira, S. Kounev, A. Avritzer, and B. D. Payne, "Evaluating computer intrusion detection systems: a survey of common practices," *ACM Computing Surveys*, vol. 48, no. 1, Article no. 12, 2015.

[29] N. K. Thanigaivelan, E. Nigussie, R. K. Kanth, S. Virtanen, and J. Isoaho, "Distributed internal anomaly detection system for Internet-of-Things," in *Proceedings of 2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, Las Vegas, NV, 2016, pp. 319-320.

[30] G. Han, J. Jiang, W. Shen, L. Shu, and J. Rodrigues, "IDSEP: a novel intrusion detection scheme based on energy prediction in cluster-based wireless sensor networks," *IET Information Security*, vol. 7, no. 2, pp. 97- 105, 2013.

[31] T. Sherasiya, H. Upadhyay, and H. B. Patel, "A survey: intrusion detection system for Internet of Things," *International Journal of Computer Science and Engineering*, vol. 5, no. 2, pp. 91-98, 2016.

[32] I. Alqassem and D. Svetinovic, "A taxonomy of security and privacy requirements for the Internet of Things (IoT)," in *Proceedings of 2014 IEEE International Conference on Industrial Engineering and Engineering Management*, Bandar Sunway, Malaysia, 2014, pp. 1244-1248.

[33] H. A. Abdul-Ghani and D. Konstantas, "A comprehensive study of security and privacy guidelines, threats, and countermeasures: an IoT perspective," *Journal of Sensor and Actuator Networks*, vol. 8, no. 2, p. 22, 2019.

[34] B. Halak, M. Zwolinski, and M. S. Mispan, "Overview of PUF-based hardware security solutions for the internet of things," in *Proceedings of 2016 IEEE 59th International Midwest Symposium on Circuits and Systems (MWSCAS)*, Abu Dhabi, United Arab Emirates, 2016, pp. 1-4.

[35] P. Sethi and S. R. Sarangi, "Internet of Things: architectures, protocols, and applications," *Journal of Electrical and Computer Engineering*, vol. 2017, article no. 9324035, 2017.

[36] D. M. Mendez, I. Papapanagiotou, and B. Yang, "Internet of Things: survey on security and privacy," 2017 [Online]. Available: https://arxiv.org/abs/1707.01879.

[37] B. B. Zarpelao, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, "A survey of intrusion detection in Internet of Things," *Journal of Network and Computer Applications*, vol. 84, pp. 25-37, 2017.

[38] K. Xing, F. Liu, X. Cheng, and D. H. C. Du, "Real-time detection of clone attacks in wireless sensor networks," in *Proceedings of 2008 The 28th International Conference on Distributed Computing Systems*, Beijing, China, 2008, pp. 3-10.

[39] R. P. Kurbah and B. Sharma, "Survey on issues in wireless sensor networks: attacks and countermeasures," *International Journal of Computer Science and Information Security*, vol. 14, no. 4, pp. 262-269, 2016.

[40] S. Fosso Wamba, A. Anand, and L. Carter, "A literature review of RFID-enabled healthcare applications and issues," *International Journal of Information Management*, vol. 33, no. 5, pp. 875-891, 2013.

[41] J. Deogirikar and A. Vidhate, "Security attacks in IoT: a survey," in *Proceedings of 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Palladam, India, 2017, pp. 32-37.

[42] M. Nawir, A. Amir, N. Yaakob, and O. B. Lynn, "Internet of Things (IoT): taxonomy of security attacks," in *Proceedings of 2016 3rd International Conference on Electronic Design (ICED)*, Phuket, Thailand, 2016, pp. 321-326.

[43] J. Singh, T. Pasquier, J. Bacon, H. Ko, and D. Eyers, "Twenty security considerations for cloud-supported Internet of Things," *IEEE Internet of Things Journal*, vol. 3, no. 3, pp. 269-284, 2016.

[44] A. Patel, S. Jain, and S. K. Shandilya, "Data of semantic web as unit of knowledge," *Journal of Web Engineering*, vol. 17, no. 8, pp. 647-674,

2018.

[45] D. Jankowski and M. Amanowicz, “Intrusion detection in Software Defined Networks with self-organized maps,” *Journal of Telecommunications and Information Technology*, vol. 4, pp. 3-9, 2015.

[46] D. Jankowski and M. Amanowicz, “On efficiency of selected machine learning algorithms for intrusion detection in Software Defined Networks,” *International Journal of Electronics and Telecommunications*, vol. 62, no. 3, pp. 247-252, 2016.

[47] S. Rathore, P. K. Sharma, V. Loia, Y. S. Jeong, and J. H. Park, “Social network security: issues, challenges, threats, and solutions,” *Information Sciences*, vol. 421, pp. 43-69, 2017.

[48] S. Hameed, F. I. Khan, and B. Hameed, “Understanding security requirements and challenges in Internet of Things (IoT): a review,” *Journal of Computer Networks and Communications*, vol. 2019, article no. 9629381, 2019.

[49] S. Hameed, U. M. Jamali, and A. Samad, “Integrity protection of NDEF message with flexible and enhanced NFC signature records,” in *Proceedings of 2015 IEEE Trustcom/BigDataSE/ISPA*, Helsinki, Finland, 2015, pp. 368-375.

[50] C. Liu, C. Yang, X. Zhang, and J. Chen, “External integrity verification for outsourced big data in cloud and IoT: a big picture,” *Future Generation Computer Systems*, vol. 49, pp. 58-67, 2015.

[51] Q. Gou, L. Yan, Y. Liu, and Y. Li, “Construction and strategies in IoT security system,” in *Proceedings of 2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing*, Beijing, China, 2013, pp. 1129-1132.

[52] S. K. Singh, S. Rathore, and J. H. Park, “BlockIoTIntelligence: a blockchain-enabled intelligent IoT architecture with artificial intelligence,” *Future Generation Computer Systems*, vol. 110, pp. 721-743, 2020.

[53] I. R. Chen, J. Guo, D. C. Wang, J. J. P. Tsai, H. Al-Hamadi, and I. You, “Trust-based service management for mobile cloud IoT systems,” *IEEE Transactions on Network and Service Management*, vol. 16, no. 1, pp. 246- 263, 2019.

[54] Z. Zhang, J. Jing, X. Wang, K. K. R. Choo, and B. B. Gupta, “A crowdsourcing method for online social networks security assessment based on human-centric computing,” *Human-centric Computing and Information Sciences*, vol. 10, Article no. 23, 2020.

[55] L. Megouache, A. Zitouni, and M. Djoudi, “Ensuring user authentication and data integrity in multi-cloud environment,” *Human-centric Computing and Information Sciences*, vol. 10, Article no, 15, 2020.

[56] A. Abubakar and B. Pranggono, “Machine learning based intrusion detection system for software defined networks,” in *Proceedings of 2017 7th International Conference on Emerging Security Technologies (EST)*, Canterbury, UK, 2017, pp. 138-143.

[57] S. K. Singh, Y. S. Jeong, and J. H. Park, “A deep learning-based IoT-oriented infrastructure for secure smart city,” *Sustainable Cities and Society*, vol. 60, article no. 102252, 2020.

[58] Y. S. Jeong and J. H. Park, “Security, privacy, and efficiency of sustainable computing for future smart cities,” *Journal of Information Processing Systems*, vol. 16, no. 1, pp. 1-5, 2020.