International Journal of Latest Engineering Science (IJLES) E-ISSN: 2581-6659

DOI: 10.51386/25816659/ijles-v4i5p101

Volume: 04 Issue: 05 **September to October 2021** **www.ijlesjournal.org**

A Technical Survey on Anomaly Detection in IOT Environment

N.Sridhar[1], Mrs.K.Shanmugapriya[2]

[1]PG Scholar, [2]Assistant Professor, Department of Computer Science and Engineering, Nandha Engineering College, Erode, Tamil Nadu, India.

ABSTRACT - *Internet of things (IoT) is an interconnected plan which advances consistent data trade between gadgets (e.g., brilliant home sensors, natural sensors, car and street side sensors, clinical gadgets, modern robots and observation gadgets). Subsequently, enormous intricacy will emerge to keep up with the future IoT foundations, which thusly prompts bothersome weakness to the framework. An anomaly detection, defined as any adjustment of normal conduct, can give early admonition of an issue. By using various machine learning algorithm that to identify assaults during runtime and take less handling time contrasted with different procedures.*

Keywords – *Anomaly Detection, Identify unusual events, Abnormal patterns, Protecting privacy, Fog Computing.*

1. INTRODUCTION

Internet of Things (IoT) is the systems administration of actual items that contain hardware installed inside the design to convey and detect associations among one another or regarding the outside climate. In the impending years, IoT-based innovation will offer progressed levels of administrations and basically change the manner in which individuals lead their regular routines. Progressions in medication, power, quality treatments, horticulture, keen urban communities, and keen homes are only a not very many of the clear cut models where IoT is unequivocally established. Over 9 billion 'Things' (actual items) are at present associated with the Internet, at this point. Soon, this number is relied upon to ascend to an incredible 20 billion. In other words, the all around the world decision innovation going about as a solitary key to contracting this entire universe to a minuscule internationally associated town, though IoT includes only two words which unequivocally portrays its definition.

1.1 IOT COMPONENTS:

There are four fundamental parts utilized in IoT:

Low-power embedded systems: Less battery utilization, superior are the converse elements assume a huge part during the plan of electronic frameworks.

Cloud computing: Data gathered through IoT gadgets is enormous and this data must be put away on a dependable stockpiling worker. This is the place where distributed computing becomes an integral factor. The data is handled and picked up, giving more space for us to find where things like electrical deficiencies/blunders are inside the framework.

Availability of big data: To realize that IoT depends intensely on sensors, particularly continuous. As these electronic gadgets spread all through each field, their use will trigger a gigantic motion of big data.

Networking connection: To impart, web network is an unquestionable requirement where each actual item is addressed by an IP address. Be that as it may, there are just a set number of addresses accessible as per the IP naming. Because of the developing number of gadgets, this naming framework won't be doable any longer. Thusly, scientists are searching for one more elective naming framework to address each actual article.

DOI: 10.51386/25816659/ijles-v4i5p101
Volume: 04 Issue: 05 September to October 2021 www.ijlesjournal.org

1.2 TWO WAYS OF BUILDING IOT:

First reason: (Real-time data): Indeed, know this as the as a matter of first importance step to start. Constant data is the unforeseen or impromptu data which is to be gathered, handled and to be conveyed quickly right away. Example: In Traffic observing framework, continuous data assumes a main part.

Second reason: (Intelligent action) In the event that user wish to diminish the human observing and are generally enamored with mechanizing everything to make item/administration to be a benchmark, then, at that point user can utilize IoT innovation. Think about a model: If the users are occupied with a pinnacle strained work and continually entering home at late evening. To settle this, imagine the cooling framework consequently turns on before the person who has entered the home and makes cool after their appearance.

1.3. IOT ENABLERS

Sensors: Gadgets which changes over actual boundaries like temperature, movement and so forth… into the electrical signs .Smart sensors are the vital empowering agents of IoT.

Actuators: Gadgets which is a difference to sensors. It changes electrical signs into actual developments. The two sensors and actuators are transducers which changes one type of energy over to other. Trade of data is the main key factor in IoT. Henceforth sensors and actuators assume an imperative part here.

RFID Tags: Remote computer chips utilized for programmed extraordinary ID of anything by labeling it over them. It has been seen it in charge cards, auto start scratches, etc.

1.4. CHALLENGES IN WORLD OF IOT

The Internet Of Things has been confronting numerous regions like Information Technology, Healthcare, Data Analytics and Agriculture. The fundamental spotlight is on ensuring protection as it is the essential justification behind different difficulties including government investment.

1.5. ANOMALY DETECTION

An anomaly, characterized as any adjustment of normal conduct, can give early admonition of an issue. For instance, abnormalities in an Internet of Things (IoT) sensor's timeseries information can show a disappointment in an assembling unit. In any case, identifying irregularities progressively is turning out to be increasingly difficult.

2. LITERATURE SURVEY

J. Santos, P. Leroux, T. Wauters, B. Volckaert, and F. D. Turck [1], concentrates on the Traditional peculiarity location approaches don't appear to be proper for delay-delicate IoT applications since these methodologies region unit extensively wedged by idleness. With the appearance of 5G organizations and by taking advantage of the advantages of ongoing ideal models, similar to Software-Defined Networking (SDN), Network perform Virtualization (NFV) and edge figuring, adaptable, low-inactivity peculiarity location becomes conceivable. This paper, partner peculiarity recognition goal for great town applications is offered, that have some expertise in low-power Fog Computing arrangements and assessed among the extent of Antwerp's town of Things testbed. A gathered monstrous dataset, the principal adequate Low Power Wide space Network (LPWAN) innovations for great town use case region unit researched.

Ibrahim Alrashdi, Ali Alqazzaz, Raed Alharthi, Esam Aloufi, Mohamed Zohdy and Hua Ming [2], introduced the loT digital protection dangers in a shrewd city, an Anomaly Detection IoT (AD-IoT) framework, which is an astute inconsistency discovery dependent on Random Forest machine learning algorithm. Their proposed

DOI: 10.51386/25816659/ijles-v4i5p101
Volume: 04 Issue: 05 September to October 2021 www.ijlesjournal.org

arrangement can viably distinguish compromised loT gadgets at conveyed haze hubs. This strategy used present day dataset to represent the model's precision. The AD-loT can successfully accomplish most noteworthy characterization precision of 99.34% with least false positive rate.

Jadel Alsamiri, Khalid Alsubhi [3], assessing different machine learning algorithms that can be utilized to rapidly and viably recognize IoT network assaults. A new dataset, Bot-IoT, is utilized to assess various detection algorithms. The seven diverse machine learning algorithms were utilized, and the vast majority of them accomplished superior. New elements were extricated from the Bot-IoT dataset during the execution and contrasted and considers from from the literature, and the new features gave better results.

Md Mamunur Rashid, Joarder Kamruzzaman, Mohammad Mehedi Hassan, Tasadduq Imam and Steven Gordon [4], presents an an attack and anomaly detection technique method dependent on machine learning algorithms (LR, SVM, DT, RF, ANN and KNN) to guard against and relieve IoT network safety dangers in a smart city. Additionally investigate gathering strategies like bagging, boosting and stacking to upgrade the exhibition of the recognition framework. Exploratory outcomes with the new assault dataset show that the proposed procedure can viably distinguish cyberattacks and the stacking troupe model outflanks similar models as far as exactness, accuracy, review and F1-Score, inferring the guarantee of stacking in this space.

Nanda Kumar Thanigaivelan, Ethiopia Nigussie , Seppo Virtanen, and Jouni Isoaho [5], proposes an novel RPL control message, Distress Propagation Object (DPO), is detailed and utilized for reporting the anomaly and network exercises to the parent hub and the router. The framework has configurable profile settings and can learn and separate between the hubs typical and dubious exercises without a requirement for earlier information. It has various subsystems and activity stages that are conveyed in both the hubs and switch, which follow up on information connection and organization layers. The framework utilizes network fingerprinting to know about changes in network geography and estimated danger areas with no help from a situating subsystem. The framework was assessed utilizing proving ground comprising of Zolertia hubs and in house created Panda Board based entryway just as environment of Cooja. The assessment uncovered that the framework has low energy utilization overhead and quick reaction. The framework involves 3.3 KB of ROM and 0.86 KB of RAM for its activities. Security examination affirms hubs response against unusual hubs and fruitful identification of bundle flooding, specific sending, and clone assaults. The framework's false positive rate assessment shows that the proposed framework displayed 5% to 10% lower false positive rate contrasted with simple detection framework.

Zhongguo Yang , Irshad Ahmed Abbasi , Elfatih Elmubarak Mustafa, Sikandar Ali [6],presents a time series include extractor (Tsfresh) and a genetic algorithm-based element choice technique are applied to quickly extricate prevailing aspects which go about as portrayal for the stream information designs. Moreover, stream information and different productive algorithms are gathered chronicled information. A quick grouping model dependent on XGBoost is prepared to record stream information components to identify suitable ADS powerfully at run-time. These strategies help to pick appropriate assistance and their separate arrangement dependent on the examples of stream information. The provisions used to portray and reflect time-series information's inherent qualities. Therefore, tests are led to assess the viability of provisions shut by hereditary algorithm. Experimentations on both artificial and real datasets exhibit that the exactness of proposed strategy beats different progressed approaches and can pick suitable assistance in various situations proficiently.

Xiali Wang and Xiang Lu [7], proposed a model to couple the Extreme Gradient Boosting (XGBoost) model and the Long Short-Term Memory (LSTM) model together for the strange state investigation on the IoT gadgets. The framework call grouping as the indicators of abnormal behaviors. The gathered framework call successions are right off the bat prepared by the popular n-gram model, which is utilized for have based interruption identifications. Then, at that point, the proposed stacking model is utilized to distinguish unusual practices concealed in the framework call successions. To assess the exhibition of the proposed model, a genuine setting IP camera framework and spot a few run of the mill IoT assaults on the casualty IP camera. Broad trial

DOI: 10.51386/25816659/ijles-v4i5p101
Volume: 04 Issue: 05 September to October 2021 www.ijlesjournal.org

assessments show that the stacking model has beated other existing abnormality discovery arrangements, and accomplish a 0.983 AUC score in certifiable information. Mathematical testing shows that the XGBoost-LSTM stacking model has astounding execution, strength, and the capacity of speculation.

Milos Savic, Milan Lukic, Dragan Danilovic, Zarko Bodroski, Dragana Bajovic , Ivan Mezei , Dejan Vukobratovic , Srdjan Skrbic and Dusan Jakovetic [8],explored the forthcoming flood of 5G IoT availability in mechanical conditions, to coordinate a DL-based inconsistency identification (AD) as a help into the 3GPP versatile cell IoT engineering. The proposed design implants autoencoder based inconsistency recognition modules both at the IoT gadgets (ADM-EDGE) and in the versatile center organization (ADMFOG), in this manner adjusting between the framework responsiveness and exactness. Configuration, incorporate, demonstrate and evaluate a testbed that executes the above assistance real- world deployment integrated inside the 3GPP Narrow-Band IoT (NBIoT) versatile administrator organization.

Gregor Cerar, Halil Yetgin, Blaz Bertalani c [9], by a genuine world exploratory IoT arrangement, four sorts of remote organization irregularities that are distinguished at the connection layer. The presentation of edge and machine learning (ML)- based classifiers to consequently identify these abnormalities. The general exhibition of three regulated and three unaided ML strategies on both non-encoded and encoded (auto-encoder) highlight portrayals. By and large, 0.90, and ii) OC-SVM beats the wide range of various solo ML approaches coming to at F1 scores of 0.99 for Sudden D, 0.95 for SuddenR, 0.93 for Insta D and 0.95 for Slow D.

Ruba abu khurma, Heba al harahsheh and Ahmad sharieh[10], presents an Anomaly Detection System (ADS) is proposed in a keen medical clinic IoT framework for distinguishing occasions of interest about patients' wellbeing and environment and, simultaneously, for network interruptions. A solitary framework to arrange foundation oversight and e-health checking has been displayed to improve assets and implement the framework dependability. Therefore, choices with respect to patients' consideration and their surroundings' variation are more precise. The low dormancy is guaranteed, an organization on the edge to take into consideration a preparing near information sources. The proposed ADS is carried out and assessed while utilizing Contiki Cooja test system and the e-wellbeing occasion identification depends on a sensible informational collection investigation. The outcomes show a high identification precision for both e-health related occasions and IoT network interruptions.

Geethapriya Thamilarasu [11], proposed a smart intrusion-detection system customized to the IoT environment. A deep-learning algorithm to recognize malignant traffic in IoT organizations. The detection arrangement gives security as a service and works with interoperability between different organization correspondence conventions utilized in IoT. The proposed detection structure utilizing both genuine organization follows for giving a proof of idea, and utilizing reenactment for giving proof of its versatility. The test outcomes attest that the proposed intrusion-detection system can perceive genuine intrusions effectively.

Faisal Hussain , Syed Ghazanfar Abbas , Ivan Miguel Pires, Ghalib A .Shah , Ubaid U. Fayyaz , Farrukh Shahzad , Nuno M. Garcia and Eftim Zdravevski E [12], proposed system comprises of an open-source IoT information generator tool named IoTFlock. The IoT-Flock tool permits specialists to foster an IoT use-case contained both ordinary and malevolent IoT gadgets and produce traffic. Also, the proposed system gives an open-source utility to changing over the caught traffic created by IoT-Flock into an IoT dataset. Utilizing the proposed structure produced an IoT healthcare dataset which contains both ordinary and IoT assault traffic. The applied diverse AI strategies to the produced dataset used to identify the cyber-attacks and shield the healthcare framework from cyber-attacks. The proposed system will help in fostering the setting mindful IoT security arrangements, particularly for a delicate use case like IoT healthcare environment.

Ismael Essop , José C. Ribeiro , Maria Papaioannou , Georgios Zachos , Georgios Mantas and Jonathan

DOI: 10.51386/25816659/ijles-v4i5p101
Volume: 04 Issue: 05 September to October 2021 www.ijlesjournal.org

Rodriguez [13], proposed there is a urgent requirement for novel security instruments. There is an absence of modern, agent, and all around organized IoT/IIoT-specific datasets which are freely accessible and comprise benchmark datasets for preparing and assessing machine learning models utilized in AIDSs for IoT/IIoT networks. The Cooja test system is utilized, in a precise way, to produce far reaching IoT/IIoT datasets. In this paper, the methodology that followed to produce an underlying arrangement of harmless and malevolent IoT/IIoT datasets. The created IIoT-specific data was caught from the Contiki module "powertrace" and the Cooja tool "Radio messages".

V. Priya , I. Sumaiya Thaseen , Thippa Reddy, Mohamed K. Aboudaif [14], proposed , the goal is to foster a two-stage anomaly detection model to upgrade the dependability of an IIoT organization. In the main stage, SVM and Naïve Bayes, are incorporated utilizing a troupe mixing procedure. K-crease cross-approval is performed while preparing the information with various preparing and testing proportions to acquire advanced preparing and test sets. Group mixing utilizes an arbitrary woodland procedure to foresee class marks. An Artificial Neural Network (ANN) classifier that utilizes the Adam enhancer to accomplish better precision is likewise utilized for forecast. In the subsequent stage, both the ANN and arbitrary woods results are taken care of to the model's grouping unit, and the most noteworthy exactness esteem is viewed as the end-product. The proposed model is tried on standard IoT assault datasets, such as, WUSTL_IIOT-2018, N_BaIoT, and Bot_IoT. The most elevated precision acquired is almost all the way. A relative examination of the proposed model utilizing best in class gathering methods is performed to exhibit the predominance of the outcomes. The outcomes additionally show that the proposed model beats conventional methods and hence works on the dependability of an IIoT organization.

Xiang Yu, Hui Lu, Xianfei Yang, Ying Chen, Haifeng Song, Jianhua Li and Wei Shi [15], proposes an unsupervised anomaly detection strategy in Internet of Things through remote sensor networks. This technique represents both a powerful anomaly status and connections between's inconsistencies based logically on their spatial and worldly neighbors. The viability of the proposed technique in an anomaly detection model. The test results show that this technique can precisely and proficiently recognize individual oddities as well as anomalous events.

Tianlong Yu, Yuqiong Sun, Susanta Nanda, Vyas Sekar, Srinivasan Seshan [16],presented that dissimilar to broadly useful computing devices, the ordinary conduct of an IoT gadget is restricted (e.g., a camera has zooming-in, video web based and sound recording practices). In light of this knowledge, conduct peculiarity recognition at the network layer. Planning such a framework is trying on two fronts. Initial, a conduct model to extract the vital attributes of IoT-explicit practices (e.g., orders or contentions utilized) from network traffic. Second, in functional undertaking environment, the organization follows for learning ordinary conduct models are unlabeled and possibly contaminated. These difficulties in planning RADAR, a pragmatic and vigorous conduct inconsistency discovery framework for big business IoT devices. A novel learning mechanism that can assemble harmless conduct models (limited state-machines) for IoT devices, from unlabeled and conceivably dirtied network follows. This methodology accomplishes high location exactness (F-Score improved by 5X contrasting and different methodologies) and is vigorous to contaminated conduct tests (F-Score>0.9 when 15% of the organization traffic of IoT devices is dirtied).

Sowmya Ramapatruni, Sandeep Nair Narayanan, Anupam Joshi, Sudip Mittal,and Karuna Joshi [17],proposed the utilization of big data and machine learning to distinguish anomalous exercises that can happen in a smart home environment. A Hidden Markov Model (HMM) is prepared on network level sensor data, made from a test bed with different sensors and smart gadgets. The produced HMM model is displayed to accomplish an exactness of 97% in distinguishing potential inconsistencies that demonstrate assaults.

Perekebode Amangele, Martin J. Reed, Mays Al-Naday , Nikolaos Thomos , Mateusz Nowak [18], investigates the utilization of machine learning strategies for anomaly detection in network traffic of an IoT network that is

DOI: 10.51386/25816659/ijles-v4i5p101
Volume: 04 Issue: 05 September to October 2021 www.ijlesjournal.org

associated through a Software Defined Network (SDN). The utilization of SDN permits a progressive approach to machine learning fully intent on reducing the packet level preparing of anomaly detection at the edge through applying extra unified machine learning in the SDN regulator. For assessment, a few supervised classification algorithms utilizing an openly accessible dataset. The outcomes support a decision-tree based approach and show that the proposed arrangement guarantees an impressive decrease in the per-packet processing at the network edge contrasted with a single stage classifier.

Rabie A. Ramadan and Kusum Yadav [19], proposes a hybrid IDS system where a pre-processing stage is used to reduce the necessary time and feature selection just as the classification is done in a different stage. The feature selection process is finished by utilizing the Enhanced Shuffled Frog Leaping (ESFL) algorithm and the chose highlights are arranged utilizing Light Convolutional Neural Network with Gated Recurrent Neural Network (LCNN-GRNN) algorithm. This two-stage technique is contrasted with cutting-edge strategies utilized for intrusion detection and it over performs them as far as precision and running time because of the light processing needed by the proposed strategy.

Elike Hodo, Xavier Bellekens, Andrew Hamilton, Pierre-Louis Dubouilh, Ephraim Iorkyase, Christos Tachtatzis and Robert Atkinson [20],proposed a threat analysis of the IoT and utilizations an Artificial Neural Network (ANN) to battle these threats. A multi-level perceptron, a kind of regulated ANN, is prepared utilizing internet packet traces, then, at that point, is evaluated on its capacity to foil Distributed Denial of Service (DDoS/DoS) assaults. This paper centers around the characterization of ordinary and threat designs on an IoT Network. The ANN system is approved against a reproduced IoT organization. The trial results exhibit 99.4% accuracy and can effectively recognize different DDoS/DoS assaults.

3. COMPARATIVE ANALYSIS

Title	Techniques & Mechanisms	Parameter Analysis	Future Work
Anomaly detection for Smart-City applications over 5G Low Power Wide Area Networks	Birch clustering and RC outlier anomaly detection mechanisms	Identify unusual events, Abnormal patterns	LPWAN technologies will be deployed
AD-IoT: Anomaly Detection of IoT Cyber-attacks in Smart City Using Machine Learning	Random Forest machine learning algorithm.	Detect compromised IoT devices at distributed fog nodes.	Developing the final model with more classification algorithms such as Conventional Neural Network (CNN).
Internet of Things Cyber Attacks Detection using Machine Learning	Machine learning methods: Random Forest Regressor algorithm	Detect IoT network attacks by using machine learning methods	Combine different machine learning algorithms as a multi-layered model to improve the detection performance
Cyber-attacks Detection in IoT-Based Smart City Applications Using Machine Learning Techniques	Information gain based feature selection technique	Defend against and mitigate IoT cyber-security threats in a smart city	Deep learning techniques to further enhance IoT attack detection performance
Hybrid Internal Anomaly Detection System for IoT: Reactive Nodes with Cross-Layer Operation	Novel RPL control message, Distress Propagation Object (DPO)	Low energy consumption overhead and fast response	Analysis of networks consisting of many nodes

DOI: 10.51386/25816659/ijles-v4i5p101

Volume: 04 Issue: 05 **September to October 2021** **www.ijlesjournal.org**

An Anomaly Detection Algorithm Selection Service for IoT Stream Data Based on Tsfresh Tool and Genetic Algorithm	Time-series feature extractor (Tsfresh), Genetic algorithm-based feature selection	Service selection method to select and configure ADS at run-time	Improve the accuracy of a service selection process .
A Host-Based anomaly Detection Framework Using XG-Boost and LSTM for IoT Devices	Extreme Gradient Boosting (XG-Boost) model and the Long Short-Term Memory (LSTM) model	Intrusion detection system (IDS) designed to identify device- or host-oriented attacks	Adjusting the parameters of this model and improving the diversity of the dataset.
Deep Learning Anomaly Detection for Cellular IoT with Applications in Smart Logistics	Anomaly Detection using ADM-EDGE and ADM-FOG, 3GPP Narrow-Band IoT	Detect anomalies	Edge devices will be explored, as well as opportunities to integrate advanced distributed learning concepts such as federated learning
Learning to Detect Anomalous Wireless Links in IoT Networks	ML techniques, Auto-encoders, Anomaly definitions	Anomalies in wireless links	Improve the accuracy in unsupervised ones reaching scores.
Efficient Anomaly Detection for Smart Hospital IoT Systems	Intrusion Detection Component (IDC), Event Detection Component (EDC), Anomaly Detection Rate (ADR)	E-health monitoring and infrastructure supervision	Developing models for detecting other specific internal attacks, such as local repair attack.
Towards Deep-Learning-Driven Intrusion Detection for the Internet of Things	Intrusion-Detection Framework, Detection Using Deep Learning	Machine-learning-based intrusion detection for resource-constrained	IDS to detect other types of attacks such as cloning of device ID, spoofing
A Framework for Malicious Traffic Detection in IoT Healthcare Environment	Machine learning techniques, IoT healthcare dataset	Detect the cyber-attacks and protect the healthcare system from cyber-attacks.	AI-based security solutions
Generating Datasets for Anomaly-Based Intrusion Detection Systems in IoT and Industrial IoT Networks	Machine learning techniques, Anomaly-based intrusion detection systems (AIDSs)	Multiple benign and attack, sensor measurement data, network-related information	Accurate and efficient detection of different types of attacks within an IoT/IIoT network.
Robust Attack Detection Approach for IIoT Using Ensemble Classifier	Machine learning techniques,Artificial Neural Network	Anomaly detection model to enhance the reliability of an IIoT network.	Improve the accuracy rate in future.
An adaptive method based on contextual anomaly detection in Internet of Things through wireless sensor networks	Unsupervised contextual anomaly detection method	Detect dynamic anomaly status and correlations between anomalies	Improving the ability of AEDTS on processing real time data streams and on anomaly detection in various application scenarios.
RADAR: A Robust Behavioral Anomaly Detection for IoT Devices in Enterprise Networks	Novel learning mechanism that can build benign behaviour models for IoT devices	Behavioural anomaly detection system	Anomaly detection for IoT deployments more broadly
Anomaly Detection Models for Smart Home Security	Hidden Markov Model (HMM)	Identify anomalous activities	Plan to generalize the system for more occupants.

DOI: 10.51386/25816659/ijles-v4i5p101

Volume: 04 Issue: 05 **September to October 2021** **www.ijlesjournal.org**

Hierarchical Machine Learning for IoT Anomaly Detection in SDN	Machine learning algorithms	SDN (Software Defined Network) security	Improve classifier associated with the SDN switches.
A Novel Hybrid Intrusion Detection System (IDS) for the Detection of Internet of Things (IoT) Network Attacks	Enhanced Shuffled Frog Leaping (ESFL) algorithm, Light Convolutional Neural Network with Gated Recurrent Neural Network (LCNN-GRNN) algorithm.	Intrusion detection	Clustering-based anomaly detection system with a specialized cloud-based IoT network.
Threat analysis of IoT networks Using Artificial Neural Network Intrusion Detection System	Artificial Neural Network (ANN)	Threat analysis of the IoT	Other deeper neural networks

4. CONCLUSION

Anomaly Detection plays an important role in enhancing Internet of things security and performance. This paper reviewed algorithms; techniques used for defend against and mitigate IoTcyber-security threats in a smart city of an existing attack detection mechanism. Major papers reviewed about the machine learning algorithms based on attack detection; identify unusual events, abnormal patterns, E-health monitoring andinfrastructure supervision. Considering this survey my work will be related to anomaly detection in IOT by implementing a machine learning algorithm.

REFERENCES

[1] J. Santos, P. Leroux, T. Wauters, B. Volckaert, and F. D. Turck, "Anomaly detection for smart city applications over 5g low power wide area networks," in NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium, 2018, pp. 1-9.

[2] Ibrahim Alrashdi, Ali Alqazzaz, Raed Alharthi, Esam Aloufi, Mohamed Zohdy and Hua Ming, "AD-IoT: Anomaly Detection of IoT Cyberattacks in Smart City Using Machine Learning," in Las Vegas, NV, USA IEEE International Conference on IEEE, 2019.

[3] Jadel Alsamiri1, Khalid Alsubhi2,Faculty of Computing and Information Technology King Abdulaziz University Jeddah, KSA, "Internet of Things Cyber Attacks Detection using Machine Learning," in (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 10, No. 12, 2019.

[4] Md Mamunur Rashid, Joarder Kamruzzaman, Mohammad Mehedi Hassan,Tasadduq Imam and Steven Gordon , "Cyberattacks Detection in IoT-Based Smart City Applications Using Machine Learning Techniques," in International Journal of Environmental Research and Public Health, 2020.

[5] Nanda Kumar Thanigaivelan, Ethiopia Nigussie , Seppo Virtanen, and Jouni Isoaho Department of Future Technologies, University of Turku, Finland, " Hybrid Internal Anomaly Detection System for IoT: Reactive Nodes with Cross-Layer Operation," in Hindawi Security and Communication Networks Volume 2018.

[6] Zhongguo Yang , Irshad Ahmed Abbasi , Elfatih Elmubarak Mustafa, Sikandar Ali , and Mingzhu Zhang School of Information Science and Technology, Beijing, " An Anomaly Detection Algorithm Selection Service for IoT Stream Data Based on Tsfresh Tool and Genetic Algorithm ," in Hindawi Security and Communication Networks Volume 2021.

[7] Xiali Wang and Xiang Lu 1Institute of Information Engineering, CAS, 100093, China School of Cyber Security, UCAS, 100049, China," A Host-Based Anomaly Detection Framework Using XGBoost and LSTM for IoT Devices ," Hindawi Wireless Communications and Mobile Computing Volume 2020.

[8] Milos Savic, Milan Lukic, Dragan Danilovic, Zarko Bodroski, Dragana Bajovic Member, Ivan Mezei Senior Member, Dejan Vukobratovic Senior Member, Srdjan Skrbic and Dusan Jakovetic Member ," Deep Learning Anomaly Detection for Cellular IoT with Applications in Smart Logistics ," arXiv:2102.08936v2 [cs.NI] 2 Apr 2021.

[9] Gregor Cerar, Halil Yetgin, Blaž Bertalaniˇc, and Carolina Fortuna Department of Communication Systems, Jožef Stefan Institute, SI-1000 Ljubljana, Slovenia ," Learning to Detect Anomalous Wireless Links ," in IoT Networks, arXiv:2008.05232v2 [cs.NI] 23 Nov 2020.

[10] Abdel Mlak Said, Aymen Yahyaoui and Takoua Abdellatif SERCOM Lab, University of Carthage, Carthage 1054, Tunisia ," Efficient Anomaly Detection for Smart Hospital IoT Systems ," Sensors 2021, 21, 1026.

[11] Geethapriya Thamilarasu * and Shiven Chawla School of STEM, University of Washington Bothell, Bothell, WA 98011, USA ," Towards Deep-Learning-Driven Intrusion Detection for theInternet of Things ," Sensors 2019, 19, 1977.

[12] Faisal Hussain , Syed Ghazanfar Abbas , Ghalib A. Shah , Ivan Miguel Pires , Ubaid U. Fayyaz , Farrukh Shahzad , Nuno M. Garcia and Eftim Zdravevski E , Al-Khwarizmi Institute of Computer Science (KICS), University of Engineering & Technology (UET), Lahore 54890, Pakistan ," A Framework for Malicious Traffic Detection in IoT Healthcare Environment ," Sensors 2021, 21, 3025.

[13] Ismael Essop , José C. Ribeiro , Maria Papaioannou , Georgios Zachos , Georgios Mantas and Jonathan Rodriguez , Faculty of Engineering and Science, University of Greenwich, Chatham Maritime, UK ," Anomaly-Based Intrusion Detection Systems in IoT and Industrial IoT Networks ," Sensors 2021, 21, 1528.

[14] V. Priya , I. Sumaiya Thaseen , Thippa Reddy Gadekallu , Mohamed K. Aboudaif,* and Emad Abouel Nasr School of Information Technology and Engineering, Vellore Institute of Technology, Vellore, 632014, India ," Robust Attack Detection Approach for IIoT ," Using Ensemble Classifier Computers, Materials & Continua, DOI:10.32604/cmc.2021.013852.

[15] Xiang Yu1, Hui Lu2, Xianfei Yang1, Ying Chen1, Haifeng Song1, Jianhua Li1 and Wei Shi3 ," An adaptive method based on contextual anomaly detection in Internet of Things through wireless sensor networks," International Journal of Distributed Sensor Networks 2020, Vol. 16(5).

[16] Tianlong Yu, Yuqiong Sun, Susanta Nanda, Vyas Sekar, Srinivasan Seshan Carnegie Mellon University , Pittsburgh, PA ," RADAR: A Robust Behavioral Anomaly Detection for IoTDevices in Enterprise Networks ," CMU-CyLab-19-003, May 21, 2019.

[17] Sowmya Ramapatruni, Sandeep Nair Narayanan, Sudip Mittal, Anupam Joshi, and Karuna Joshi Computer Science and Engineering, University of Maryland, Baltimore County, Baltimore, Maryland ," Anomaly Detection Models for Smart Home Security ,"in IEEE Intl Conference on Intelligent Data and Security (IDS),2019.

[18] Perekebode Amangele, Martin J. Reed, Mays Al-Naday , Nikolaos Thomos , Mateusz Nowak ,University of Essex , Poland ,UK ," Hierarchical Machine Learning for IoT Anomaly Detection in SDN ," Proceedings of the 33rd International Conference on Information Technologies (InfoTech-2019) 19-20 September 2019, Bulgaria.

[19] Rabie A. Ramadan and Kusum Yadav Computer Science and Engineering College, University of Hai'l, Hai'l, Saudi Arabia ," A Novel Hybrid Intrusion Detection System (IDS) for the Detection of Internet of Things (IoT) Network Attacks ," Annals of Emerging Technologies in Computing (AETiC) Vol. 4, No. 5, 2020.

[20] Elike Hodo, Xavier Bellekens, Andrew Hamilton, Pierre-Louis Dubouilh, Ephraim Iorkyase, Christos Tachtatzis and Robert Atkinson Department of Electronic & Electrical Engineering University of Strath clyde Glasgow, G1 1XW, UK ," Threat analysis of IoT networks Using Artificial Neural Network Intrusion Detection System ,"in International Symposium on Networks, Computers and Communications(ISNCC),2016.

