DOI: https://doi.org/10.24113/ijoscience.v8i7.489

Anomaly Detection for IOT/Cloud-Based Model in Fog Computing Using Machine Learning

Suraj Nayak
M.Tech Scholar
Oriental Institute of Science & Technology
Bhopal, Madhya Pradesh, India
srjnk27@gmail.com

Shadab Pasha Khan
Assistant Professor
Oriental Institute of Science & Technology
Bhopal, Madhya Pradesh, India

Abstract:-We know that the key technologies that are involved in the Internet of Things are wireless sensor networks and cloud computing, big data, embedded systems, and the internet. It is a giant network with connected devices. These devices gather and share data. But many IoT devices have poor security and cybercriminals are taking benefit of this. The two techniques cloud and fog computing both combined can be used to transfer secure data in IoT devices as cloud computing provides storage of data on cloud servers and fog computing offers us various services to access data and provides support for cloud servers. This research work presents various techniques to detect an intruder and anomaly detection in IoT-based cloud systems. Also, a comparison of all the techniques used to detect intruders and anomalies are compared on various parameters like accuracy, performance, efficiency, precision, recall, the detection rate.

Keywords:-Fog Computing, Cloud Computing, Internet Of Things, Intrusion Detection, Anomaly Detection.

I. INTRODUCTION

IoT (Internet of things) is a great example of this, the Internet of things has made daily life very easy and comfortable. It has made it even easier for us by using modern technologies and tools. This amazing technology is known as IoT (Internet of things). The internet of things is the technology of science, through which many technologies and devices are interconnected through the Internet. In this technology, the devices are interconnected by internet sensors. . In the meantime, the knowledge has industrialized rapidly to include social connections for, presenting a group of Internet-of-The whole lot (IoE). At contemporary, the ecosphere contains billions of calculating plans and devices that are obstinately detecting, accruing, uniting, and assessing the great amount of our individual information. Internet of things is made advanced by modern technology. [1] To use the Internet of Things, it is necessary to have general knowledge of computers and the internet, because it is a networking technology with the help of the Internet of Things (IoT) any person can connect the devices of his home with the help of the internet so that you can control all those devices from anywhere. It can be used even when the IP address of your mobile and devices are connected. Internet of Things (IoT) presentations are dissimilar then established trendy numerous areas similar home-based mechanization, business mechanization, medical care mechanization, industrial mechanization, motorized, keen vigor switch, road traffic accomplishment, and so forth. The biggest disadvantage associated with the Internet of Things is security. In today's era, many questions arise regarding the security of the Internet. In such a situation, due to connecting everything to the Internet, there will be a threat to their security. At the same time, in the coming time, this technology can also become a threat to personal things. That's the sign to classify any change in the system to deliver dependable then protected operative of the system. Furthermore, through observing stimulating or uncommon proceedings in IoT systems, the system can sidestep communicating unhelpful or mistaken dimensions. Which container decreases dynamism ingesting, in addition, to advancing the dependability of the system. The technique of perceiving motivating or infrequent occurrences in the system is identified as incongruity uncovering. To recognize irregularities in a network, it is compulsory to discover a classical for the common of ordinary information and before the irregularities can be recognized as individual's information courses that swerve meaningfully after the standard ideal.

Internet of Things (IoT) schemes remain frequently dangerous dormancy-delicate. Such evidence wants toward lightweight debauched since the substances inside the System concluded the accesses for an Internet. [1-2] For instance, as Disaster Management Internet of Things (IoT) classifications necessity notice stimulating proceedings which remain connected toward the determination aimed at remaining the IoT substructure was considered for example intensity, deluges, smoke seepage the moment conceivable besides brand unquestionable not to fail any of them owing to forthcoming irregularities. Irregularities may be confidentially hooked on two groups

1. Irregularities connected to mechanical or internal organization matters for example communiqué disappointment and noisy signals, purpose catastrophe, and breakdown.

2. Irregularities associated with organization truthfulness and sanctuary for example mischievous occurrences, invader substances. [2] The auspicious method aimed at Abnormality Uncovering in Smart Environments mendacities in retaining Machine Learning methods. These methods survey replicas that are to be learned and advance the pronouncement beginning an involvement. Keen Surroundings incline in the harvest extra system streams then old-fashioned complexes, payable to the mammoth ruler for shrewd campaigns in the system, as well as the various types of applications in these devices. Hence, the monitoring of these network currents produces a huge capacity of information, assembly the presentation for fogging and utility calculating indispensable to this situation [3].

Defending IoT strategies and the entree system accountable for transferring valuable information concerning the fog necessitates extenuation of occurrences similar to Denel of services, docks scanning, system perusing, important movements, then showy troop. [5] Occurrences from IoT strategies pointing the admission system resolve, not individual disturb facilities that guzzle information from IoT systems nonetheless also place into inquiry the consistency of the admittance system. Making a protected beside IoT outbreaks is challenging outstanding to the gauge of the mechanisms in the IoT system and the capacity of information impending since the IoT policies.

Researchers in further arenas like computer sciences treated various methods to identify anomaly detection consuming Users' data over the internet in fog computing. An adequate investigation has been done by many researchers to narrate machine learning techniques to detect anomalies in IoT-based out assist devices by using various remarkable techniques are discussed in this research paper [7]. The main aim is to improve computerized tools by providing work for and raising machine-learning techniques along with morphological features and datasets and to identify anomaly detection in fog computing [5]. Though the researchers aimed to apply various techniques and algorithms to detect intruders in IoT devices. This technique provides the capability to study the modified detection of anomalies in the earlier stage than structures that are ready to accomplish concurrently. The problem statement and approximately connected mechanism on identifying anomaly detection are discussed in the literature review given below.

II. LITERATURE REVIEW

S. Manimurugan et al. [1] proposed an improved naive Bayes classifier that is based on a principal module study to perceive anomaly detection for cyber-crimes. In this work, the combination of the two most used techniques of IoT through fog computing and cloud computing method is established to enhance IoT applications for smart cities. To evaluate the results of proposed techniques a UNSW-N815 dataset is used to test the attacks on an anomaly detection model. The experimental result shows that the proposed INB-PCA model achieves a detection from attacks is 95 % and an accuracy of 93%. But the proposed model has limitations in that system faces some false-positive rates in anomaly detection.

YAHYAOUI et al. [2] proposed framework names such as READ-IoT, Reliable Event, and anomaly Detection framework to detect anomalies, network failure, and cyber-attacks in IoT devices while transferring data. The proposed model combines actions more on irregularities discovery in an IoT-based system based on both centralized and management perceptions. To evaluate the performance of the proposed technique it is tested using the NSL-KDD dataset to validate its effectiveness two requests are used fire detection and unlawful individual detection. The experimental result shows that the proposed READ-IoT framework authenticates the competence in rapports of occurrence discovery accuracy and actual data handling. But the proposed model has limitations in that system fails when connected among the cloud computing properties in the central system.

Moreira et al. [3] proposed ISAD an intelligent system for network anomaly detection by combining fog computing and cloud computing approaches. The proposed model services machine learning methods to comprehend the normal performance of the system currents in the keen situation, provided that firm alteration to the common besides unexpected vagaries in system performance to evaluate the performance of the proposed technique it is tested by creating an artificial fog environment using Microsoft AZURE. The experimental result shows that the proposed ISAD performed better as compared to traditional techniques and achieves an accuracy of 86% in anomaly detection. But the proposed model has limitations as it requires a large amount of audit data to perform outcomes.

Chatterjee et al. [4] proposed a hierarchical approach based on fog computing to detect anomalies in Phasor Measurement Units (PMU's) for distributed detection in fog computing. Now their projected method, Phasor Measurement Units (PMU's) indications by alike manner outlines stood gathered at a fog bulge where information retrieval was achieved using a Vigorous Phasor Measurement Units (PMU's) -founded process. The experimental result shows that the proposed model achieves an average MSE of 2.46e, Maximum MSE of 1.55e. But the proposed model has limitations as it is prominent to unlikely errors in judgment creation.

Lingjuan et al. [5] proposed an innovative irregularity uncovering technique, named Fog-Authorised irregularity discovery, based on binding the dispensation control of the fogging podium and using a competent overexcited gathering procedure. To evaluate the performance of the proposed method is tested using amalgamation and real data set which shows proposed system achieves 82% accuracy a noteworthy decrease in terms of latency and vigor feasting. But the proposed model has limitations as in a distributed environment very less events are taken for each fog node which can be stimulating.

MILOS et al. [6] proposed an anomaly detection technique based on deep learning in a 3GPP mobile IoT manner. The

proposed method consists of an auto encoder-established anomaly detection component for both IoT policies (ADM-EDGE) also for fundamental mobile systems (ADM-FOG). The result of the proposed work shows the precision is 0.705, recall 0.690, and FI score 0.697. But the proposed model has limitations in that it is not good for large-scale locations.

Moustafa et al. [7] proposed a method known as Outlier Dirichlet Combination- FLIERS (ODM-ADS) for anomaly discovery grounded on confrontational arithmetical learning instruments. Performance to evaluate the performance of the proposed technique is tested under two cases regular and regular with an attack data marker. The experimental result shows that the proposed model achieves disaster recovery of 96% accuracy of 97% and final performance review 0.46% which shows that the ODM-ADS technique has a faster processing speed in terms of time complexity.

QAISAR et al. [8] proposed an introduction and anomaly detection system (IDPs) based on cloud-helped software-defined network (SDN) for IoT devices. The main objective of this proposed method is to detect time analysis of various attacks and intrusion detection systems in fog/IoT-based systems. The experimental result shows that the proposed model achieves precision 97%, recall 95% Fi-score 96%, and accuracy 98%. The proposed work demonstrates the usefulness of different clusterings after consuming dissimilar space dimensions.

Radwa EI et al. [9] proposed an approach to sense irregularities in the superiority of the Smart Network using a Fog figuring method founded on the Open-Fog Orientation Construction (RA) which is a general Fog stage that is intended to be appropriate to any marketplace arena or request.

Jaiswal et al. [10] proposed a hierarchically Scattered Fogging design to organize machine learning founded irregularity discovery replicas for producing visions from the composed Keen rhythm device information. The result of the proposed method designates its considerable probable as an applied system to be rummage-sale further in Smart Network checking and present time irregularity discovery As it is clear from the result that it takes Prediction of 16 Hours, Linear Regression 38% Support Vector 36% Regression Random 48% and Forest Regression Gradient Boosting Regression 53%.

Zeke et al. [11] proposed a phase measurement unit (PMU) by using two anomaly detection techniques single spectrum analysis and K-nearest neighboring (KNN) in edge fog hierarchy clustering architecture to detect anomalies more accurately. Tested consequences of the proposed model show that together approaches are appropriate at the cloud sheet with dissimilar benefits and restraints. (Nader et al. [12]) Fogging might overtake some of the restrictions for cloud computing by contribution facility which can be evaluated on fog nodes that seems nearer to the IoT devices also in the arena of the tenders, delivers provision for flowing, flexibility, position consciousness, squat latency, and immediate obligation.

Below in table 1 assessment of IoT based systems for anomaly detection is presented. Whereas in table 2 some major contributions of researchers for IoT based intrusion detection are discussed.

Fig 1 shows the graph representation accuracy, Detection Rates= (DR), False Positive Rates= (FPR), of various techniques used to detect anomalies. It is clear from the graph that accuracy of PMU fog is highest among all other techniques.

Table 1: Assessment of anomaly detection techniques in IoT-based systems.

Ref	Approach	Description
[13]	State transition analysis	Simulations diffusions as a sequence of state deviations that main from an original protected formal to a mark cooperated formally. As state transition diagrams are used which represents the pictorial structure of penetrations to detect an intruder
[14]	Sequence matching and learning	Proposed an approach that uses a hypothesis in which an operator replies predictably in a frequent order. This method absorbs distinguishing orders of activities produced from the operator side.
[15]	Predictive pattern generation	In this method, prediction is done based on events that have previously ensued. An occasion is highlighted as invasive such as the L.H.S side of the instruction remains co-ordinated, then the correct side is statistically divergent from the forecast.
[16]	Keystroke Monitoring	Keystroke Monitoring is known for the procedure used toward interpretation or greatest together the Keystrokes arrived from operator's side which in a replay to the system throughout a communicating assembly.
[17]	Statistical	The statistical methods describe the standard or predictable performance by gathering information relating to the performance of genuine operators ended a dated of time. Numerical examinations are then practical to the experiential performance to control the legality of the performance.

Table 2: A Comparisons of Anomaly detection of various techniques

Ref	Technique Used	Accuracy	Detection Rate	Limitations
[1]	INB	92.48	95.35	faces some false-positive rates in anomaly detection
[2]	READ-IoT	98	89.4	fails when connected among the cloud computing properties in the central system.
[3]	ISAD	96	87	As it requires a large amount of audit data to perform outcomes.
[6]	ADM-EDGE ADM-FOG	91.7	88	That it is not good for large-scale locations.
[7]	ODM-ADS	98.59	98.25	It has high computational time
[8]	IDPS	98.25	84	That it is not good for large-scale locations.
[11]	PMU fog	94.29	89.2	It has high computational time

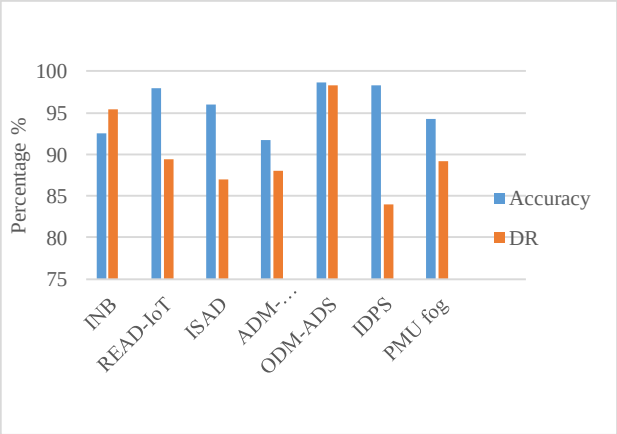

Fig 1: Graph of accuracy and detection rate of various techniques

III. CONCLUSION

In this research paper, various methods used to detect anomalies for IoT-based applications in Fog/Cloud computing are discussed. Various techniques are enlightened to detect intruders and anomalies with their comparisons of accuracy, computation time, and time to detect anomalies are discussed. Also, this paper offers a comprehensive review and analysis of the best significant current development algorithms for anomaly detection in fog computing. The proposed technique.

REFERENCES

[1] J. P. Anderson, "Computer security threat monitoring and surveillance," Tech. Rep. James P Anderson Co Fort Washingt. Pa, p. 56, 1980, doi: citeulike-article-id:592588.

[2] R. Heady, G. Luger, A. Maccabe, and M. Servilla, "The architecture of a network level intrusion detection system," 1990, doi: 10.2172/425295.

[3] G. Sai Nikhil, A. S. Rajasekaran, M. Parimala, and S. Velliangiri, "Applications of Machine Learning in Anomaly Detection," Lect. Notes Electr. Eng., vol. 834, pp. 491–499, 2022, doi: 10.1007/978-981-16-8484-5_48.

[4] M. Hasan, M. Islam, I. Islam, and M. M. A. Hashem, "Attack and Anomaly Detection in IoT Sensors in IoT Sites Using Machine Learning Approaches," p. 100059, 2019, doi: 10.1016/j.iot.2019.100059.

[5] E. Biermann, E. Cloete, and L. M. Venter, "A comparison of Intrusion Detection systems," Comput. Secur., vol. 20, no. 8, pp. 676–683, 2001, doi: https://doi.org/10.1016/S0167-4048(01)00806-9.

[6] Z. Yang, N. Chen, Y. Chen, and N. Zhou, "A Novel PMU Fog Based Early Anomaly Detection for an Efficient Wide Area PMU Network," in 2018 IEEE 2nd International Conference on Fog and Edge Computing (ICFEC), 2018, pp. 1–10. doi: 10.1109/CFEC.2018.8358730.

[7] R. Jaiswal, A. Chakravorty, and C. Rong, "Distributed Fog Computing Architecture for Real-Time Anomaly Detection in Smart Meter Data," in 2020 IEEE Sixth International Conference on Big Data Computing Service and Applications (BigDataService), 2020, pp. 1–8. doi: 10.1109/BigDataService49289.2020.00009.

[8] R. El-Awadi, A. Fernández-Vilas, and R. P. Díaz Redondo, "Fog Computing Solution for Distributed Anomaly Detection in Smart Grids," in 2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 2019, pp. 348–353. doi: 10.1109/WiMOB.2019.8923222.

[9] Q. Shafi, A. Basit, S. Qaisar, A. Koay, and I. Welch, "Fog-Assisted SDN Controlled Framework for Enduring Anomaly Detection in an IoT Network," IEEE Access, vol. 6, pp. 73713–73723, 2018, doi: 10.1109/ACCESS.2018.2884293.

[10] N. Moustafa, K.-K. R. Choo, I. Radwan, and S. Camtepe, "Outlier Dirichlet Mixture Mechanism: Adversarial Statistical Learning for Anomaly Detection in the Fog," IEEE Trans. Inf. Forensics Secur., vol. 14, no. 8, pp. 1975–1987, 2019, doi: 10.1109/TIFS.2018.2890808.

[11] M. Savic et al., "Deep Learning Anomaly Detection for Cellular IoT with Applications in Smart Logistics," IEEE Access, vol. 9, no. 833828, pp. 59406–59419, 2021, doi: 10.1109/ACCESS.2021.3072916.

[12] L. Lyu, J. Jin, S. Rajasegarar, X. He, and M. Palaniswami, "Fog-Empowered Anomaly Detection in IoT Using Hyperellipsoidal Clustering," IEEE Internet Things J., vol. 4, no. 5, pp. 1174–1184, 2017, doi: 10.1109/JIOT.2017.2709942.

[13] K. Chatterjee and N. R. Chaudhuri, "Distributed Anomaly Detection and PMU Data Recovery in a Fog-computing-WAMS Paradigm," in 2020 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), 2020, pp. 1–6. doi: 10.1109/SmartGridComm47815.2020.9302971.

[14] A. Yahyaoui, T. Abdellatif, S. Yangui, and R. Attia, "READ-IoT: Reliable Event and Anomaly Detection Framework for the Internet of Things," IEEE Access, vol. 9, pp. 24168–24186, 2021, doi: 10.1109/ACCESS.2021.3056149.

[15] S. Manimurugan, "IoT-Fog-Cloud model for anomaly detection using improved Naïve Bayes and principal component analysis," J. Ambient Intell. Humaniz. Comput., 2021, doi: 10.1007/s12652-020-02723-3.

[16] D. A. B. Moreira, H. P. Marques, W. L. Costa, J. Celestino, R. L. Gomes, and M. Nogueira, "Anomaly Detection in Smart Environments using AI over Fog and Cloud Computing," in 2021 IEEE 18th Annual Consumer Communications Networking Conference (CCNC), 2021, pp. 1–2. doi: 10.1109/CCNC49032.2021.9369449.